United States Treasury

Financial Management Service

Paper Check Conversion

Standard Operating Procedures

and

User's Manual

Version 2.3.0.2838

Military POS, MVD and Lockbox

Revised October 8, 2003

United States Treasury

Check Point of Sale and Central Image & Research Archive Installation & User Guide

Manual Contents

Section Title	Responsible Party
Installation and Configuration	System Administrator
Daily Processing Step-By-Step User Guide	System Administrator, Cashier
Master Verification Database (MVD) & Central Image & Research Archive (CIRA)	System Administrator
Reporting and Balancing with CA$H-LINK	System Administrator, Cashier
Personnel Change Over	System Administrator, Cashier
Troubleshooting	System Administrator, Cashier
Appendix	System Administrator, Cashier

Introduction

What is Paper Check Conversion (PCC)?

Paper Check Conversion (PCC) is the process of converting paper checks presented to agencies into electronic ACH debits to the check writer's account. The process works as a Point of Sale (POS) when the consumer presents a physical check to the cashier for payment, or as an Accounts Receivable/Lockbox when the check is received through the mail as payment and the writer of the check is not present. The cashier takes the completed check and inserts it into the Point-of-Sale scanner that reads the MICR line on the bottom of the check and captures the image of the check into the POS computer. The check image is forwarded and stored in a central database called the Central Image and Research Archive (CIRA). When processing as a POS, the cashier returns the cancelled check to the consumer on the spot with the transaction information. The financial information captured from the MICR line is transmitted to the Federal Reserve Bank of Cleveland (FRBC). FRBC settles the transaction through the ACH network, makes CA$H-LINK entries, and provides electronic deposit ticket and/or debit voucher (returns) (SF215 and SF5515) reporting back to the collection site.

The PCC process involves the following major components:

Point of Sale (POS)

The software to capture and forward the image of the check and the information from the transaction is called the POS. Depending on the respective agency's needs, the POS will also collect relative payment information. The agency will determine on an overall agency basis which information is necessary. Refer to the Installation and Configuration section for setup and configuration of the POS using the PCC SAT and PCC POS systems and setup of the POS scanner. Refer to the Daily Processing sections for POS operating instructions.

Accounts Receivable/Lockbox

This is an optional feature. Accounts Receivable/Lockbox is a processing mode that is used when checks are mailed and the writer of the check is not present. For more information, refer to the Installation and Configuration and Daily Processing sections of this manual.

Central Image and Research Archive (CIRA)

The POS application transmits all the image transaction information to Central Image and Research Archive (CIRA). The CIRA online repository is a database of all transactions processed electronically. It allows authorized users to perform research on a specific item, or on a group of items, using your web browser. . The CIRA can only be accessed by authorized people within the agency as well as authorized staff at the Federal Reserve Bank of Cleveland (FRBC). Refer to the CIRA section for information on accessing and researching transactions through the web site.

Settlement and Reporting

The Federal Reserve Bank of Cleveland will convert the financial information captured from each check that was forwarded to the CIRA to an electronic Automated Clearing House (ACH) item. The FedACH system is used by the Federal Reserve to settle ACH items between financial institutions. (As this system is internal to the Federal Reserve Bank, no further reference will be provided in this manual.)

Master Verification Database (MVD)/Local Verification Database (LVD)

The Master Verification Database (MVD), provides the POS system information to ensure a presented check is acceptable. The verification database is an online database that maintains the agency hierarchy check cashing policy, dishonored check information, and manually entered blocked items based on an agency's policy. The Master Verification Database (MVD) provides downloads of negative check information and blocked items to the POS daily to the Local Verification Database (LVD). The LVD is a verification database that resides on each POS terminal. The information in the LVD prevents checks being cashed on accounts, or other agencies specified criteria, that is a violation of the agency's policy. Verification information is available online. The MVD can be manually updated by the Federal Reserve Bank of Cleveland (FRBC) and selected agency personnel determined by each agency. If the agency utilizes the MVD and LVD, refer to the Master Verification Database section for more information.

This is an optional function. The verification database box must be checked on the PCC SAT System Configuration screen, as described in the Installation and Configuration section, to utilize this function.

Location Group Management

The MVD restricts the display of data based on the location of the user. A user will only see records, which are associated with locations at or below the user's location in the hierarchy or at locations specified in the Location Group. Depending on the type of data being requested, different rules will apply, as appropriate. Refer to the Master Verification Database section for more information.

CA$H-LINK

The CA$H-LINK system is used to settle and report transactions for the U.S. Government. This system will reflect deposits for all checks processed as well as debits for checks that are returned to an agency. Each day the Disbursing Officer, or designated receiver, will receive a report via email that details transactions that have posted to CA$H-LINK. Refer to the Reporting and Balancing with CA$H-LINK section for more information.

POS Diagram

The following diagram depicts the flow of transactions through the Paper Check Conversion process conducted through the POS:
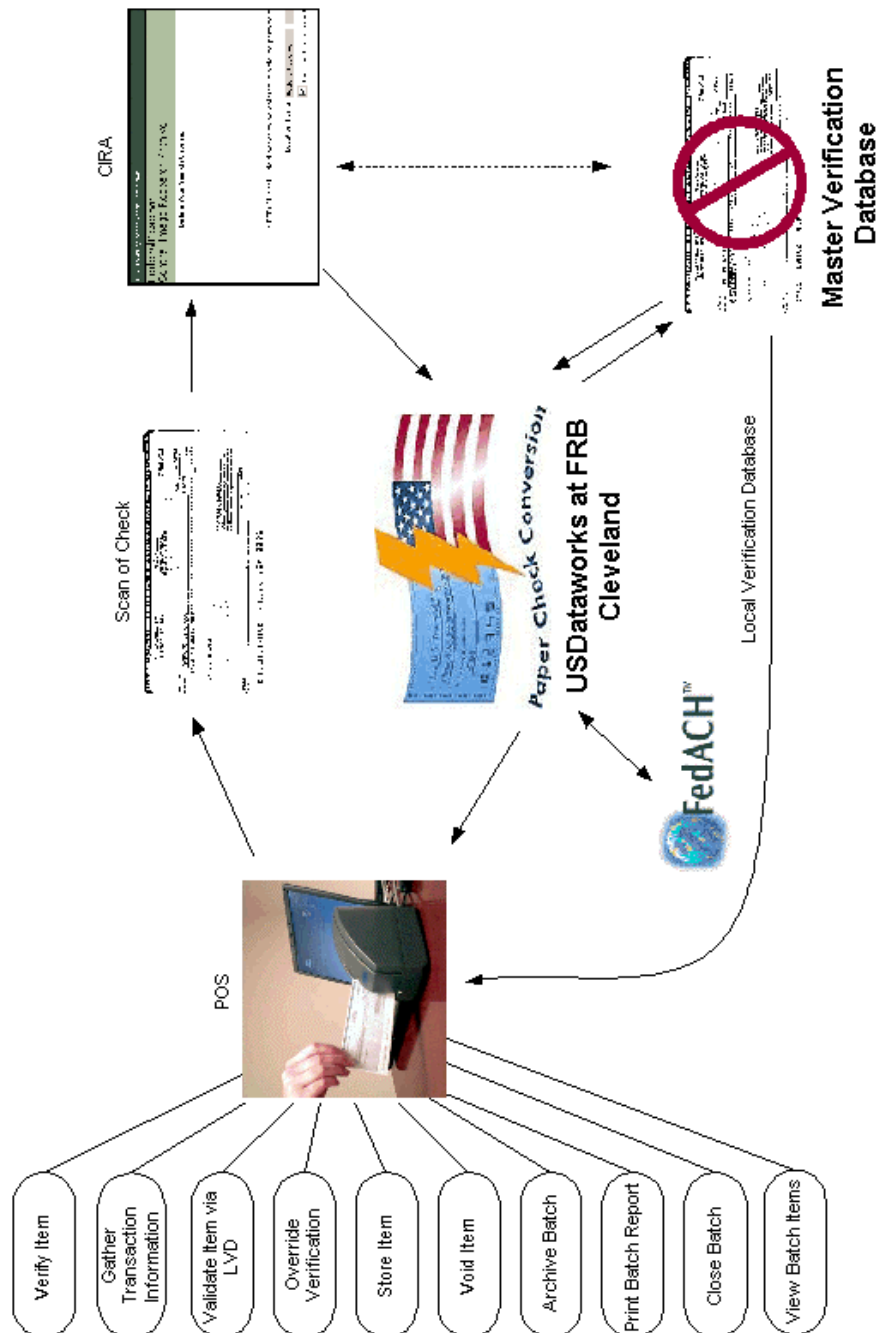
United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Installation and Configuration

Version 2.3.0.2838

Revised October 8 , 2003

TABLE OF CONTENTS

Installation & Configuration

Note: This section may be used by the System Administrator to follow for first time installation.

Requirements and Configuration

Computer Requirements

- 10GB Hard Drive
- Minimum of 128MB RAM
- Minimum Pentium 500 MHz computer
- Available 9 pin serial port to connect POS Scanner
- 1 available PCMCIA slot (for instances where PCC will be installed on laptops) or a zip drive attached via parallel port
- CD-ROM drive
- Local or LAN printer
- Standard RJ45 Ethernet connection
- POS will need Microsoft Internet Explorer Version 6.0 or higher (preferred browser) with 128-bit encryption installed or Netscape Navigator 6.22 or higher.
- POS application requires the Microsoft Database Engine (MSDE) and will install it as required

Service Pack 3 for upgrading the SQL2000 Desktop Engine (MSDE) optional (POS version 2.2.0.0523 only) POS version 2.3.0.2838 includes SP3 for SQL:2000

Supported operating systems are Windows NT, 2000 – Service Pack 2, and XP

Router/Firewall Requirements

Router/Firewall administrators must ensure and verify via outbound and inbound ACL's that complete https access, on port 443, exists between each POS site and the PCC/MVD/CIRA PRODUCTION located at IP 199.169.194.27. The IP address for contingency is 199.169.192.11. Full upload and download capability using https is required to operate the PCC system.

Example ACL for both router and firewall access:

- **Access list XXXX permit tcp (Agency Internet IP Address-Proxy or Translated) host 199.169.194.27 eq 443.**

There is more security by dedicating a direct connection from an Agency IP address to the MVD IP address. This mechanism can ensure that any desktop running the PCC system can secure access to the MVD/CIRA as long as there are no group or user restrictions applied. Once the IP address is requested, it should be translated at the firewall to the agency IP address and forward the connection onto the MVD/CIRA. Also, your firewall rules need to allow traffic to and from IP address 199.169.192.11 for contingency purposes. In the event that there is a problem with our primary system, the secondary system will use this IP address to connect to our backup site.

More information on the PCC system and its parts can be obtained from the Federal Reserve Bank of Cleveland at 216-579-2112 or 1-800-624-1373, or your US Treasury, FMS Point of Contact.

Scanner Hardware

The scanner hardware consists of three components. They are:
1. EC5000i scanner unit
2. 9 Pin serial data cable
3. AC adapter power brick

The scanner serial data cable plugs into both the scanner unit and the 9 pin serial connection on the laptop or PC. Plug the power unit into a surge protected power strip.

NOTE: The scanner MUST be 4 inches away from EM (Electro-magnetic) equipment, including the PC. If the scanner is too close it can cause a misread or an image distortion. These devices include the computer, credit card reader devices, laser beams from bar code scanner devices, etc.
.

On initial startup of the scanner it will cycle through each light. Upon completion, the light on the front of the scanner should be amber. If the light on the scanner is red, please refer to the Troubleshooting section in this manual.

Yes/No Keypad (Optional)

The Yes/No Keypad allows the customer to confirm the amount of the transaction. If the agency uses the Yes/No Keypad, it is enabled in the POS configuration. It is connected through the back of the scanner.

1. Connect provided scanner cable to scanner back.

2. Connect keypad cable to scanner cable.

3. Plug keypad cable into power strip.

Operating System Setup

The POS runs on the following operating systems: Windows NT, XP, and 2000 (minimum Service Pack 2 for Windows 2000).

Verify that either the laptop or desktop computer is configured with an approved Operating System. Verify that the laptop or desktop computer time and date configurations are correct. If needed, the laptop or desktop date and time can be configured by selecting the Date/Time icon located in the Windows Control Panel.

Due to the negative impact on the PCC POS performance, it is recommended that programs such as games, screensavers, etc. should not be installed on your PCC POS computer or on the laptop provided by the US Treasury (if applicable).

NOTE: All devices should be plugged into a surge protection system.

Mirror Image - Backup Device Installation

The POS requires the capability to have secondary storage. The secondary storage, or mirror image, retains the batch information and check image prior to transmission to the CIRA. The mirror image is a back-up drive in case the hard drive crashes or data on the hard drive is corrupt. Without the mirror image, daily processing information would not be retained and not be available for transmission or batch recovery in the event of a PC failure. If the above scenarios occur, call FRBC at 216-579-2112 or 800-624-1343 or DSN 510-4-2-86824, option 6, option 4, or refer to the Troubleshooting section of this manual.

Two options are available for storage device, PCMCIA Smart Media or a zip drive. The volume of items processed by your location will determine which device will serve as your backup device.

Option 1 - PCMCIA Smart Media Device

One option for storing backup data is a Smart Media device. This may already be installed in the machine in the PCMCIA slot, which is located on the left side of the laptop.

Inserted into this device is a 1.5" x 1.75" 32 or 64MB storage card (depending on your volume). If the PC hard drive fails during operation before a batch is closed and transmitted to the CIRA site, pending items can be retrieved from the storage card by using another PC with the same device.

Contingency and backup procedures are contained in the *Troubleshooting* section of this manual.

Option 2 - Zip Drive

The second backup device option available with either a laptop or a desktop is a Zip Drive. This device may be internally installed in the desktop PC or may be externally attached to the parallel port on the POS PC.

It is recommended that a 250 MB storage disk is used with the zip drive. Zip disks are also available in 100 MB. The size you choose should be based on your volume. Should the PC fail during operation before a batch is closed and transmitted to the CIRA site, pending items can be retrieved from the zip disk using another PC with the same device. An external zip drive must be installed and configured prior to the installation of the PCC POS software.

Contingency and backup procedures are contained in the *Troubleshooting* section of this manual.

NOTE: During installation, the location of the secondary drive is established as explained in the New Installation section. Go to Windows Explorer to verify that the secondary drive selected during installation indicates the device (either option 1 or 2) being used. The drive selected during software installation should also display in the System Administration Tool (SAT) system configuration.

LAN Connectivity

If the POS is connected to the agency location's LAN, the laptop or desktop must be configured as a member of the domain used at the site and added to the network. This is necessary to submit transactions, and to use any LAN–connected printers. **The ability to print is required to properly process daily work.**

New Installation

NOTE: If an error is encountered during any part of the installation, contact the FRBC at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4.

Very Important – The System ID/machine name should not be changed after the Installation of the PCC POS software. The machine name is directly tied to our PCC system and doing so will render the software unusable. If the System ID/Machine name needs to be changed it should be done prior to the installation of the PCC POS software.

1. Insert the PCC POS CD (version 2.3.0.2838)
2. Click on 'Start', select 'Run' then click Browse. Navigate to the CDROM drive, usually D:\ or E:\. Double-click the file named UST Paper Check Conversion System and from the 'Run' window, click OK.
3. If the computer does not have Microsoft Data Access Component (MDAC), a screen appears indicating that the PCC POS install requires MDAC (Microsoft Data Access Components version 2.7) to be installed (or reinstalled if the current version is lower than 2.7) This may require a reboot before the PCC POS application installation can begin.
4. If MDAC is already installed on the computer step 3 will be by-passed and the installation will begin.
5. The 'UST Paper Check Conversion System' setup window will appear. Click Next.
6. A window will appear stating that 'A new instance of MSDE (Microsoft SQL ServerDesktop Engine) needs to be installed. Would you like to install? Select Yes to install. Installation will take a few moments.
7. A UST System Information screen will appear and the user will be prompted to manually configure specific fields and selections.

NOTE: Please insert your specific agency information as explained below or call FRBC at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4, to provide your accurate agency information. It is crucial that the information in the following fields be correct.

8. Input the **required** fields & selections:
   - **Name** – Agency name or program.
   - **Organization** – Location name
   - **ALC** – Enter the respective agency's ALC + 2. ALC/DSSN code is needed to specifically identify the location of the transactions processed, POS scanner, and application. **ALCs/DSSNs have been predefined and should not be changed unless prior approval from the U.S. Treasury has been obtained and coordinated with FRBC.** Altering values set in this field will negatively impact the processing of the agency location's items.
   - **Terminal ID** – Required for each location. It is provided by FRBC and should not be changed. The naming convention for the terminal ID is *XXXXX*, in which 'xxxxx' is a numeric code assigned by FRBC to designate the terminal.
   - **Secondary Storage –** Installer should automatically select the secondary storage drive (Normally E:\ or D:\). You can change the drive by selecting Browse. Go to Windows Explorer to confirm that the proper drive is selected and coordinates with the location of the secondary storage device (PCMCIA storage card or zip drive). Daily and archived batches will be stored on this drive.
9. Click on Next.

Destination Folder Selection:
10. Installer will select the destination folder as indicated in the screen shot below. It is recommended to use pre-defined settings. Click Next.
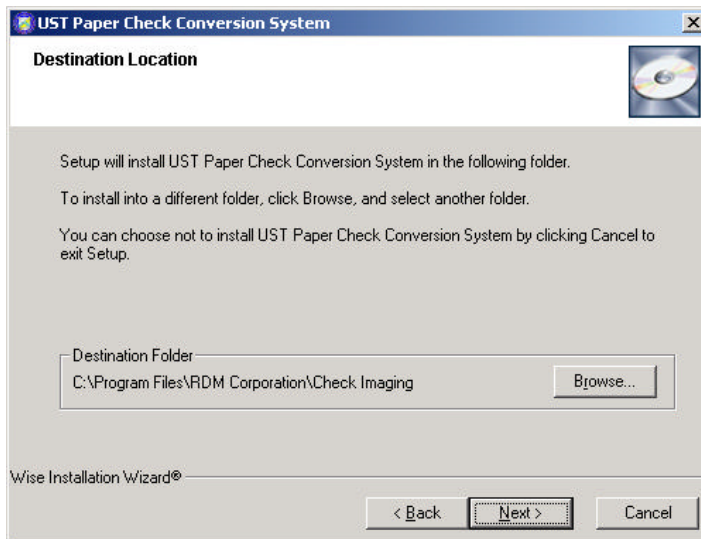
11. A 'Start Installation' window will appear. Click [Next.] The PCC POS installation will continue. This will take several minutes.

12. When the install is complete click [Finish]. Upon a successful installation, two shortcuts to the POS program (PCC POS and PCC SAT) will appear on the PC desktop.

NOTE: If the installation is unsuccessful or the application is corrupt, refer to the Troubleshooting section in this manual for instructions on reinstalling the PCC application or call FRBC at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4, for assistance on reloading the application installation.
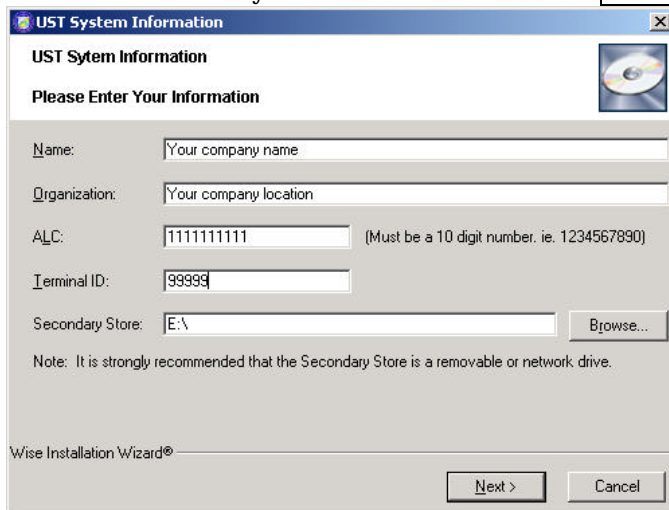
Upgrading the PCC Application

Determining the Version

1. Logon to the PCC POS application.
2. Select 'Help', then 'About PCC POS' from the menu at the top of the main POS screen. The version number displays at the top of the About PCC POS window. The current POS version is 2.3.38. When upgrading, you may need to verify this to be your current version number.
3. Select [Close] to close the window.
4. Logon to the PCC SAT application.
5. Select 'Help', then 'About PCC System Administration'. The current SAT version is 2.3.28. When upgrading, you may need to verify this to be your current version number.
6. Select [Close] to close the window.

Installing the Upgrade

When the upgrade is installed, the existing configuration and user setup is maintained.

1. Print the SAT and POS activity log for the past 90 days and user information from the SAT before upgrading the existing application. To print the activity log and user information, refer to *Activity Log and User Information* section in the *Appendix.*
2. Determine the current application version by following the steps above.
3. Launch PCC SAT and login.
4. Select File, and Configuration. Make a note of the ALC, and the Secondary Image Storage. Close the PCC SAT application.
5. Launch PCC POS and login.
6. Select File, and Configuration. Select the Application tab and make a note of the Terminal ID.
7. Close the PCC POS application.
8. Insert the CD with the POS version upgrade into the CDROM drive.
9. Select 'Start', 'Run', then 'Browse' from the application toolbar at the bottom of the desktop.
10. Select the CD-ROM drive.
11. Double-click the 'UST Paper Check Conversion System' and select OK
12. A UST Paper Check Conversion System Setup screen appears. Select Next to continue.
13. If the current version of MDAC is not present or lower than 2.7, setup will need to install it at this time. If the correct version of MDAC is detected, setup will continue with the next step.
14. A UST System Information screen will appear with your PCC information. Make sure that the information is correct – especially your ALC and terminal ID. If you are uncertain, please call the FRBC at 216-579-2112 or 800-624-1373 or DSN 510-4-2-86824, option 6, option 4, to confirm the accuracy of the information. Select Next.

15. Installer will select the destination folder as indicated in the screen shot below. It is recommended to use pre-defined settings. Click Next.
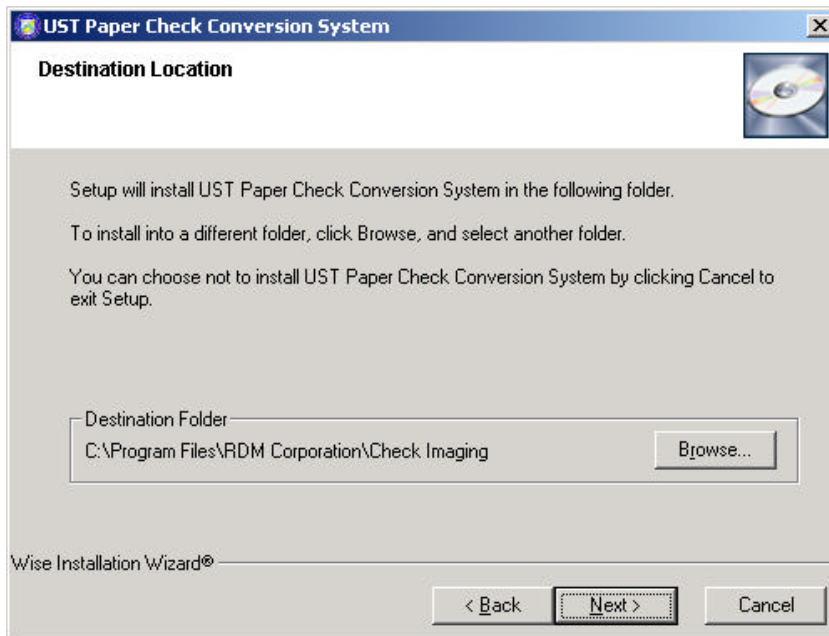
15. A 'Start Installation' window will appear. Click Next. The PCC POS installation will continue. This may take several minutes.
16. When the install is complete click Finish. Upon a successful installation, two new shortcuts icons to the POS program (PCC POS and PCC SAT) will appear on the PC desktop.

NOTE: If the installation is unsuccessful or the application is corrupt, refer to the Troubleshooting section in this manual for instructions on reinstalling the PCC application or call FRBC at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4, for assistance on reloading the application installation.
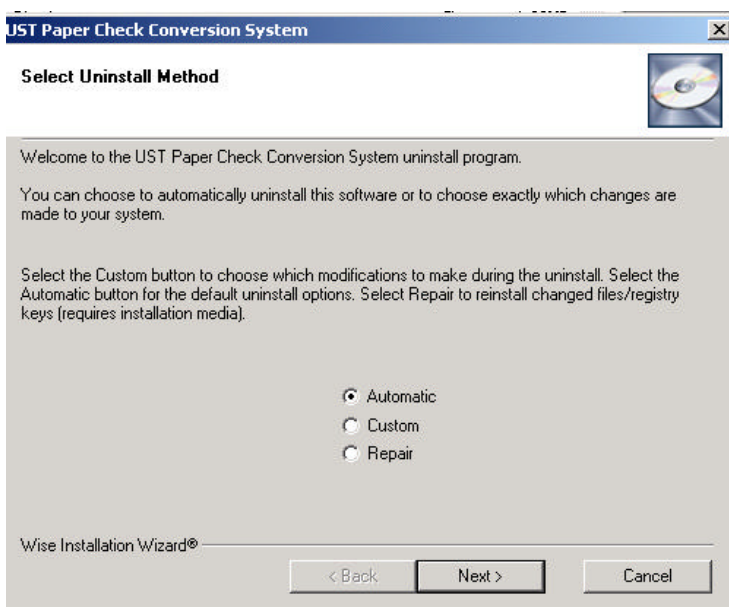
Uninstall

Note: Uninstallation of the PCC software should not be performed without permission from FRBC. Please call the PCC Customer support at 800-624-1373, 216-579-2112 or DSN 510-4-2-86824, option 6, option 4.

1. To uninstall the software, click on 'Start', 'Settings', 'Control Panel'. Double-click on 'Add/Remove Programs'.

2. Click on 'UST Paper Check Conversion System' then click on Change/Remove.
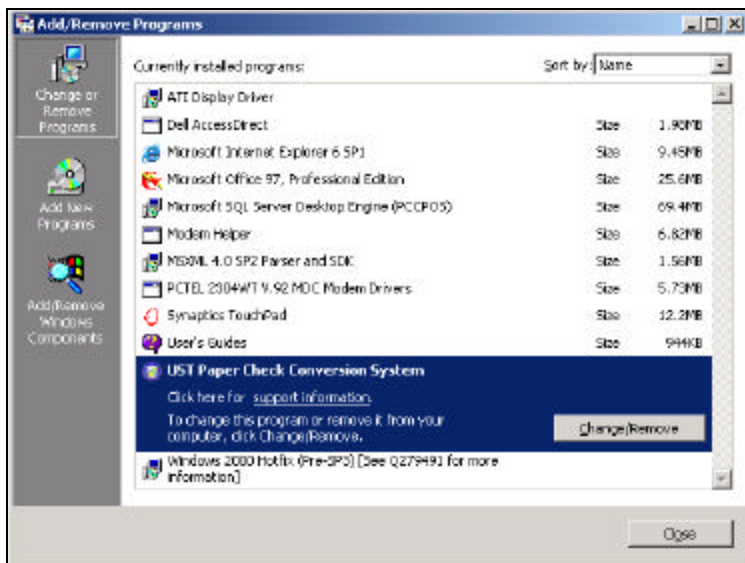
3. A 'Select Uninstall Method' window will appear and 'Automatic' should already be chosen. If not**, be certain to choose 'Automatic'** by clicking the radio button to the left of 'Automatic'. Click Next.

Note: Never use the 'Custom' uninstall. Doing so will allow a user to remove folders, system files and registry entries which can damage your operating system.

Note: Never use the 'Repair' function. Doing so may cause file corruption.

4. A prompt will appear that indicates that the uninstall process is about to begin. Click Finish.

5. The system will ask if you wish to keep the data from this product. Click Yes. This will save your user information, application defaults and un-transmitted batches

Note: If you choose No, user information, application defaults and non-transmitted batches will be lost

6. When the Uninstall process is complete, the screen will return to the Add/Remove programs window. Click on Close at the bottom right of the window. Close the Control Panel window by clicking on the 'X' in the upper right corner of the window.

Re-Install

After you have performed the Un-install procedure, the software will need to be re-installed. Follow these steps to re-install the PCC POS software.

1. Insert the PCC POS CD (version 2.3.0.2838)
2. Click on 'Start', select 'Run' then click Browse. Navigate to the CDROM drive, usually D:\ or E:\.
3. Double-click the file 'UST Paper Check Conversion System.exe. In the 'Run' window, click OK At execution, the UST Paper Check Conversion System Setup window appear. Click Next.
4. A UST System Information screen will appear and the user will be prompted to manually configure specific fields and selections (see below).

NOTE: Please insert your specific agency information as explained below or call FRBC at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4, to provide your accurate agency information. It is crucial that the information in the following fields be correct.
*.*

5. Input the **required** fields & selections:
    *   **Name** – Agency name or program.
    *   **Organization** – Location name
    *   **ALC** – Enter the respective agency's ALC + 2. ALC/DSSN code is needed to specifically identify the location of the transactions processed, POS scanner, and application. **ALCs/DSSNs have been predefined and should not be changed unless prior approval from the U.S. Treasury has been obtained and coordinated with FRBC.** Altering values set in this field will negatively impact the processing of the agency location's items.
    *   **Terminal ID** – Required for each location. It is provided by FRBC and should not be changed. The naming convention for the terminal ID is *XXXXX*, in which 'xxxxx' is a numeric code assigned by FRBC to designate the terminal.
    *   **Secondary Storage –** Installer should automatically select the secondary storage drive (Normally E:\ or D:\). You can change the drive by selecting Browse . Go to Windows Explorer to confirm that the proper drive is selected and coordinates with the location of the secondary storage device (PCMCIA storage card or zip drive). Daily and archived batches will be stored on this drive.
6. Click on Next.

Destination Folder Selection:

7. Installer will select the destination folder as indicated in the screen shot below. It is recommended to use pre-defined settings. Click Next.
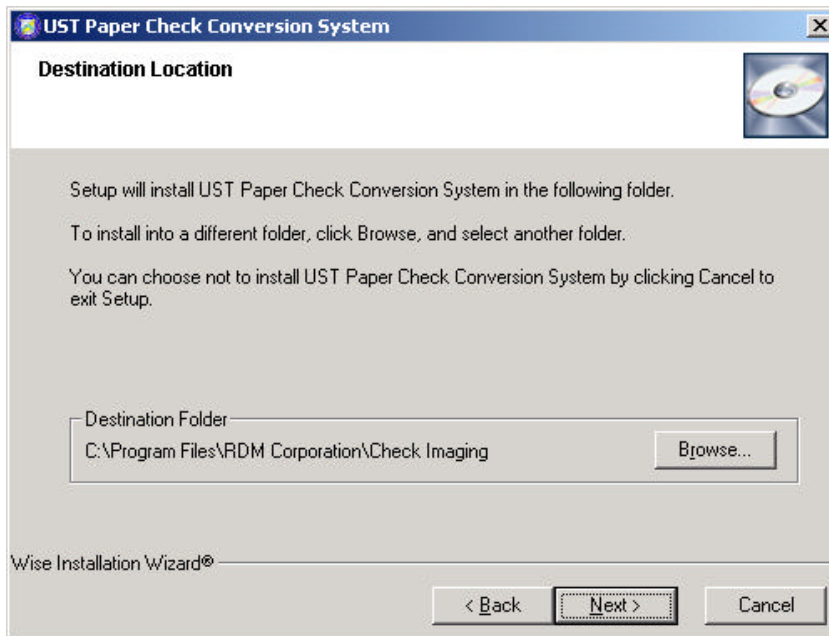
8.   A 'Start Installation' window will appear. Click [Next.] The PCC POS installation will
        continue. This could take several minutes.
9.   When the install is complete click [Finish]. Upon a successful installation, two shortcuts to
        the POS program (PCC POS and PCC SAT) will appear on the PC desktop.

***NOTE: If the installation is unsuccessful or the application is corrupt, refer to the
Troubleshooting section in this manual for instructions on reinstalling the PCC application or
call FRBC at 800-624-1373 or 216-579-2112 for assistance on reloading the application installation.***

PCC SAT – System Administration Tool

Only authorized System Administrator, IT Support or designated Point of Contacts (POC) should be accessing the PCC SAT application.

For the initial installation, the deployment specialist (i.e. FRBC or Treasury representative) will launch the PCC SAT icon to complete security and application configuration setup. If the deployment specialist is not present at the location site, call FRBC at 800-624-1373 or 216-579-2112 for assistance.

The agency's authorized user will enter the login and password provided by the deployment specialist, then press OK. The password will need to be changed upon initial login to a unique password and should only be known to users who have administrative access rights.

(Note: Once the administrative password has been changed, it should be written down and <u>locked up</u> for future use. If, at any time, the PCC SAT system cannot be accessed via the administrative logon because the password is not known, the only way to access the SAT is to uninstall and reinstall the PCC POS software. Keeping track (and tight security) of the administrative password is crucial.)

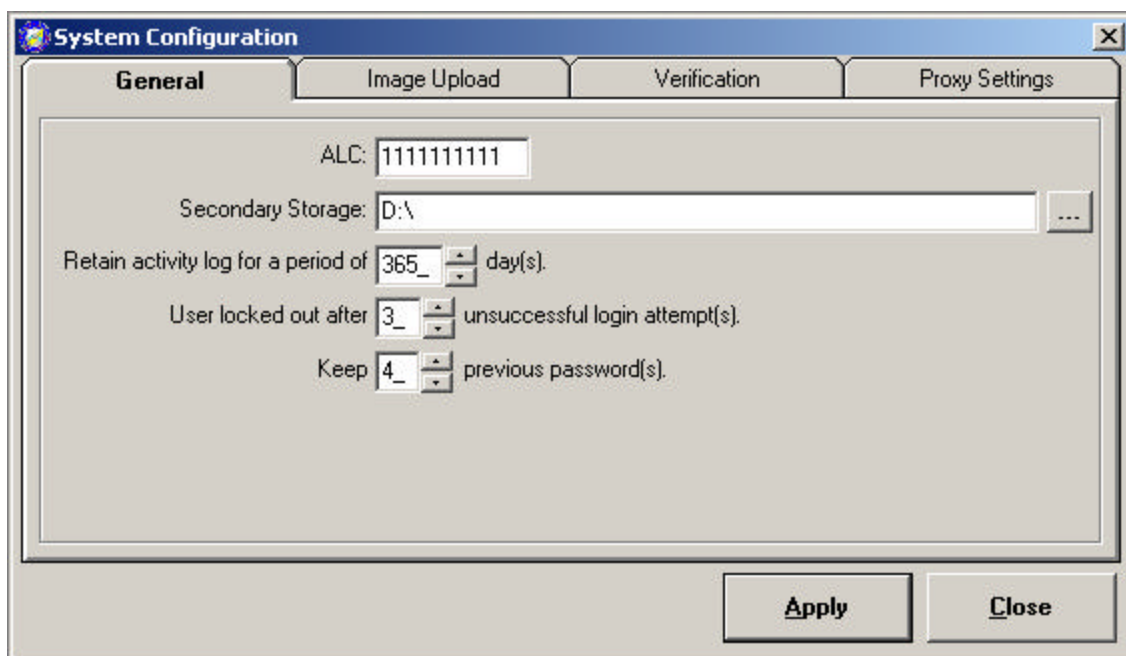The PCC SAT application consists of the following components:
- System Configuration
- User Administration
- Activity Log
- Batch Recovery
- LVD Reset (Optional for Accounts Receivable/Lockbox – may be made inactive if not used)
- Help
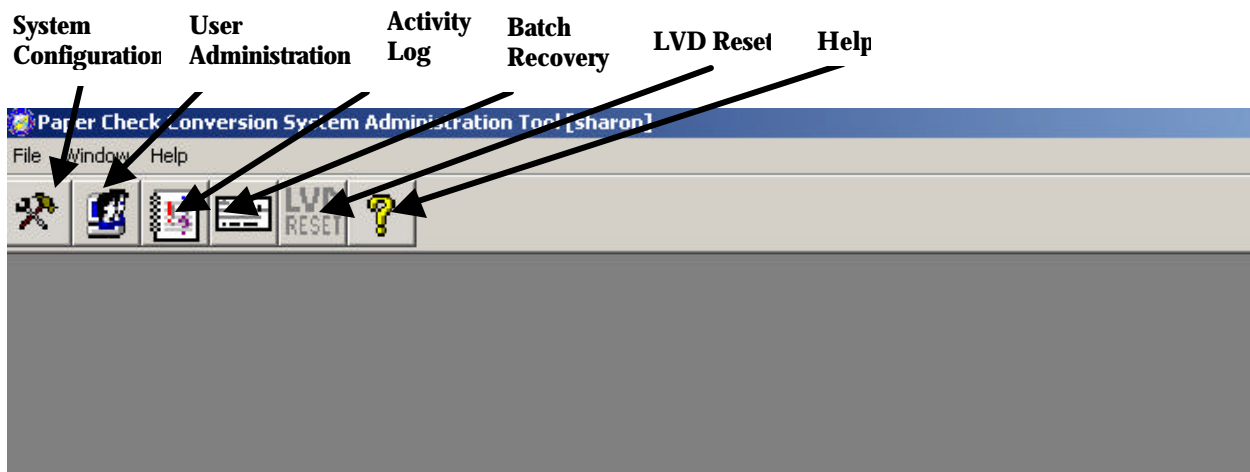
System Configuration

Select the System Configuration icon from the main PCC SAT screen.

There are four tabs on this screen and they are described below.

General

- ALC + 2 is a predefined code used to specifically identify the location of the transactions processed. This field is set during installation and should not be changed unless prior approval frm the US Treasury has been obtained and coordinated with FRBC. Verify the accuracy of the setting since this determines CA$H-LINK and accounting entries. If a PC is re-deployed to another location, the POC must change this field if the information is different than what was entered during installation. **ALCs/DSSNs have been predefined and should not be changed unless prior approval from the U.S. Treasury has been obtained and coordinated with FRBC.**

- The 'Secondary storage' field was configured during installation (PCMCIA storage card, LAN, or zip drive). The drive displayed should be the same drive that was selected during installation. Refer to the New Installation section, if needed. If the Secondary Image Storage fails while in the PCC POS application, refer to the *Troubleshooting* section.

- The 'Retain activity log' field defines the length of time the system activity is retained. The period to retain the system activity log is configurable by the number of days. It is recommended that a minimum of one year of activity be maintained.

- System access provides the ability for an administrator to lock out users after a configurable number of unsuccessful attempts. The number of previously used passwords must be

configured. Upon installation, the agency POC should confirm that setting is in compliance with the agency's guidelines.

- Set the number of previously used user passwords that are retained in the history file. Typically, three previous passwords are retained, but this setting should conform with an agency's IT security policy.

NOTE: Password administration is allowed by users that have permission to configure user roles. Authorized users are able to change and unlock user passwords by selecting the Edit User icon on the User Administration screen.

Image Upload
Configurable fields for daily batch updates. Should be set exactly as displayed below and should not be changed unless at the direction and guidance of the FRBC or the Treasury. **Upon deployment or re-installation, these settings will be confirmed. A change to any of these settings will produce a negative impact to the processing of your check items.**
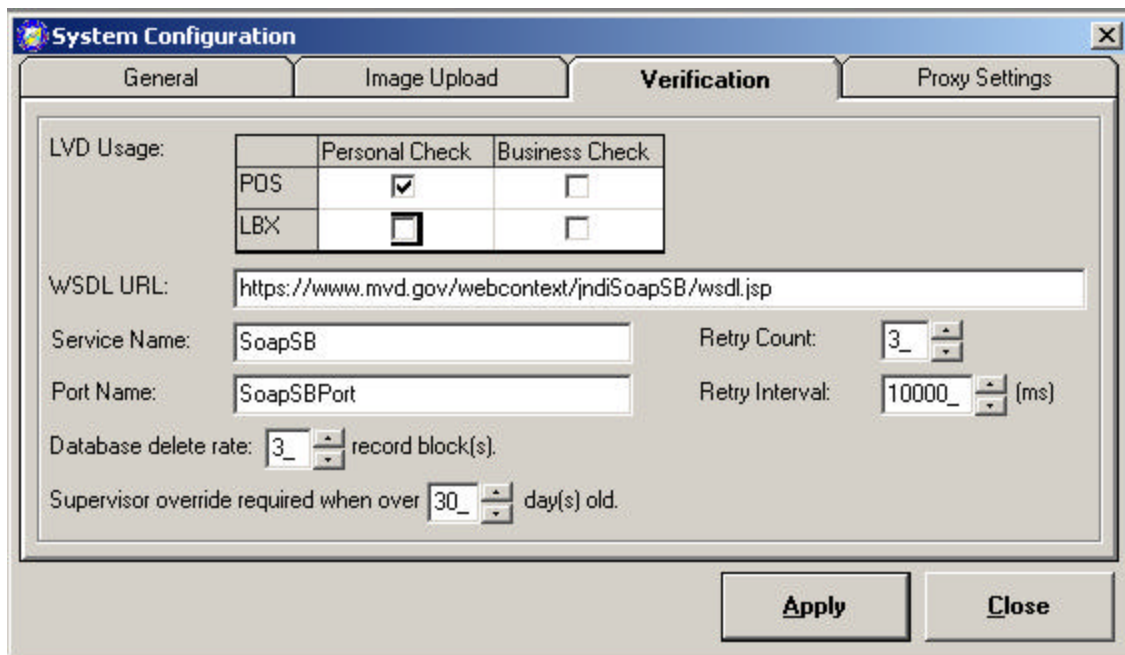

Note: The 'Password' field in the above screen needs to be reset. The deployment specialist can provide this password. If the deployment specialist is not present, call at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4.

Verification

This tab contains the configurable fields for verification updates. The LVD usage can be customized based on the type of checks/payments you accept via the PCC POS. If LBX (Lockbox) only options are chosen in the LVD usage, the Local Verification Database option will become inactive for all POS transactions, personal or business.

The WSDL URL, Service Name and Port Name are defaulted during installation and look exactly as displayed below. Upon deployment or re-installation, these settings will be confirmed. These three fields should not be changed without the direction or guidance of FRBC. A change to any of these fields will **produce a negative impact to the processing of your check items.**

The remainder of the configuration settings is set to system defaults and should not be changed.

Proxy Settings
Configurable fields are available for agencies to insert their internal proxy settings if proxy servers are used. for updating proxy settings. Use of this screen will depend upon your firewall rules. Contact your firewall administrator for further information.

Note: The PCC software is proxy aware. If your agency is proxy aware, you will need to enable the use of Proxy Server by placing a check in the box for 'Use Proxy Server'. The associated proxy server's IP address and/or port numbers need to be specified in the 'Server' field. Any required user authentication parameters needed for internet access need to be set in the 'Use Authentication' field. Your central network infrastructure staff can assist you by providing the required values needed for this screen.

User Administration

Users must be setup in the PCC SAT user administration and assigned roles and permissions before accessing the PCC POS application.

Select the User Administration icon from the main PCC SAT screen to access the following user administration screen.

New User   Edit User   Delete User   Configure System Roles   Print
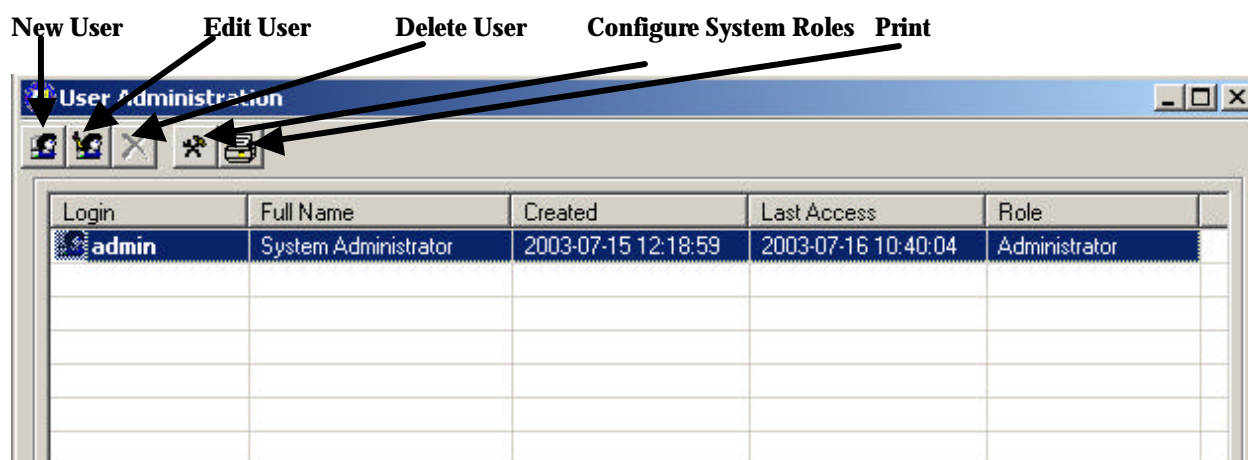
WARNING: The admin user should never be deleted from the PCC POS system.

The user administration consists of five primary functions:
- Add New User
- Edit User
- Delete Users
- Configure System Roles
- Print out a list of system users

Further explanations of these functions are covered on the next pages.
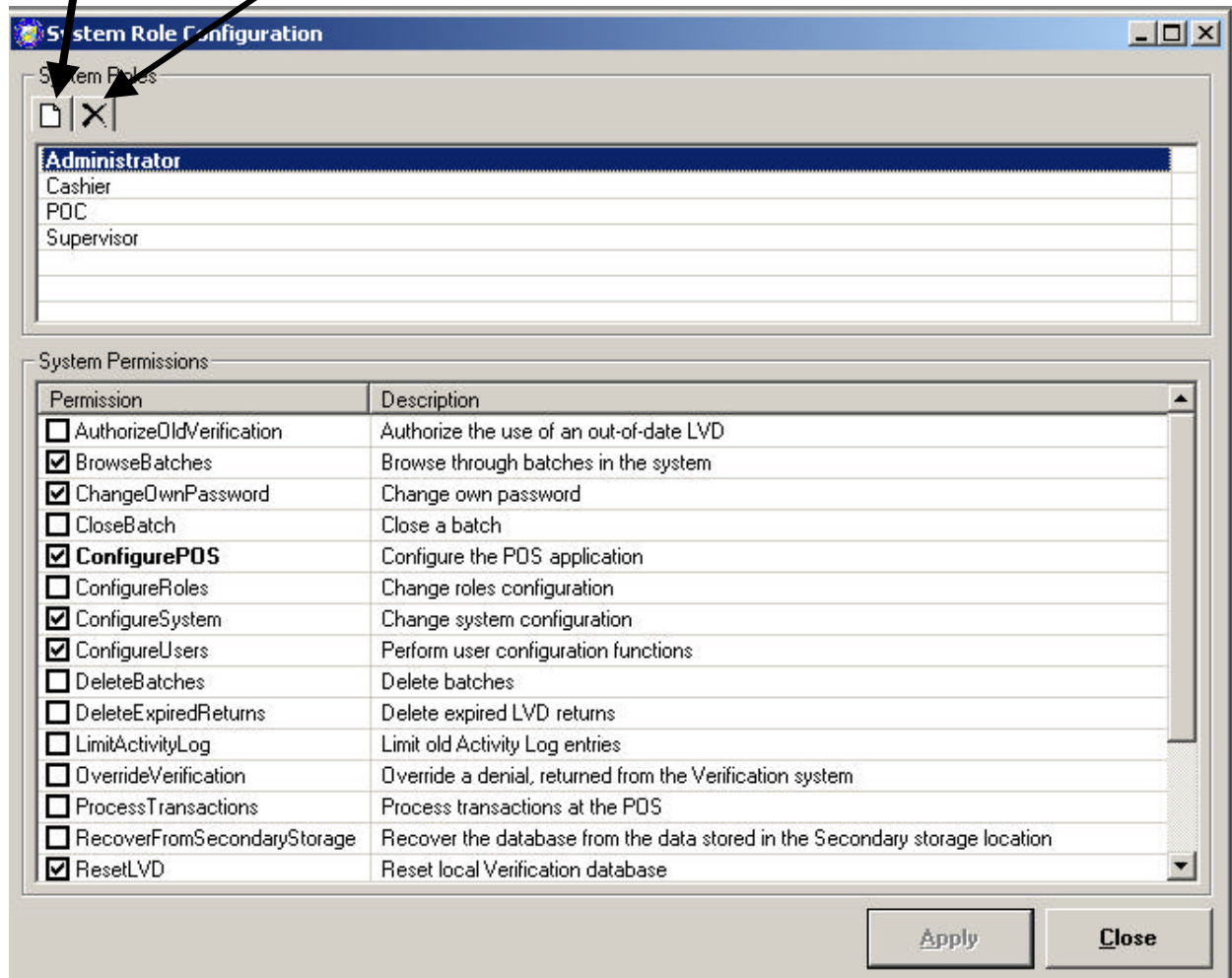
Configure System Roles
From the main PCC SAT screen, select the User Administration icon, then select the Configure System Roles icon, from the User Administration screen to configure system roles.

System permissions indicate the access of each role. Review the accuracy and completeness of the role permissions to agency requirements prior to assigning users. The 'admin' user cannot alter system roles. If system roles need to be reconfigured, a user needs to be added that has authorization to alter system roles, then that user needs to sign on and reconfigure the system roles.

Administrator, Cashier, POC (Point of Contact), and Supervisor are provided as system default roles. These roles can be changed according to your agency's needs. Additional system roles required by an agency can be added or edited by an authorized user. Roles should be consistent across an agency, and not be location specific. Highlight the specific role to determine the role permissions. For example, if you are logged in as a Supervisor, and the Supervisor role has the System Permission to configure users, the Supervisor user will be able to perform user configuration functions.
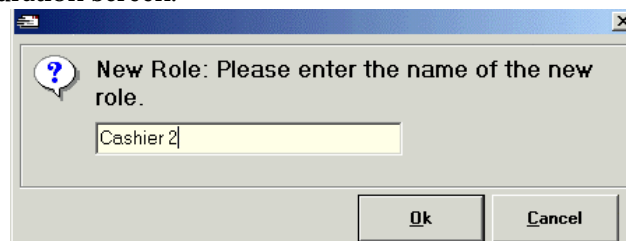
New System Role   **Delete System Role**

Adding System Roles

1. *Authorized users* are able to add system roles by selecting the New System Role button from the System Role Configuration screen.
2. Enter the system role as indicated below, then select OK. The new role will appear on the System Role Configuration screen.

3. Select the new role and check the System Permissions for that role. The System Permission, ChangeOwnPasword, must be checked for all roles. If it is not selected, the user will not be able to sign on.
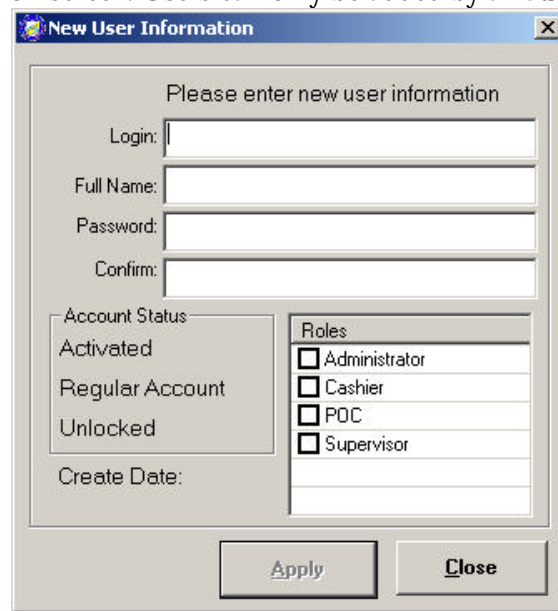
4. Select Apply.

Deleting System Roles

1. *Authorized users* are able to delete system roles by selecting the Delete System Role button from the System Role Configuration screen.
2. At the verification message, select Yes. The role will be removed from the system Role Configuration screen.

NOTE: A role cannot be deleted if a user is assigned to that role. Reassign users to new roles before deleting the existing role.

Adding a New User

From the main PCC SAT screen, select the User Administration icon, then select the New User icon from the User Administration screen. Users can only be added by an authorized administrator.

Enter the new user information including the Login, Full Name, and default Password. The default password is typed twice, once in the 'Password' field and then again in the 'Confirm' field.

*   The Login is not case sensitive and must be between four and twenty characters. The login should be identifiable by the user, for example the user's first initial and last name. The Logon should not include commas or apostrophes.
*   Passwords must be a minimum of eight alphanumeric characters, and are case sensitive. Users should be assigned a default user password since users are required to establish a new password upon their initial login.

Note: Users should be aware that 3 unsuccessful login attempts (or the configurable number of attemps that are set in the System Configuration) will result in a locked account.

Once an account is locked, an administrator must sign on to the PCC SAT and unlock the user.

Select the appropriate role, then select ⟦Apply⟧ when complete. Once a user has been added, an administrator can view the user's information, which would include the status of their account and the date that the user was added to the system.

Edit User (Unlock, Reset, Activate or Deactivate User Account)

Unlock, Activate or Deactivate
A user's account will become 'locked' if their unsuccessful login attempts exceeds the number of unsuccessful attempts as set in the System Configuration.   An administrator can 'Unlock' a user account. (Note: the user's password may also need to be reset if the user does not remember their password – see Reset Password). A user account can also be 'Deactivated' if, for example, a user is on vacation or medical leave. Upon their return, their account can be 'Reactivated'. These functions can only be performed from the User Administration screen. There are no menu options for these functions

1. From the main PCC SAT screen, select the User Administration icon.

2. The screen will display all users as seen below. When a user account is locked, a red 'lock' will appear to the left of the login name. When a user id deactivated, it will be flagged with a red arrow symbol.

Deactivated   **Locked**

3. To unlock, activate, or deactivate a user account, right-click on the user's login. A drop down menu will appear with choices as seen below.

4. Click the action you wish to take and the user's account is immediately updated.

Reset password

If a user has become locked because they cannot remember their password, the administrator not only needs to unlock the user account, but will also need to reset the user's password.

1. Click the 'User Administration' icon from the main PCC SAT screen. A window will appear that displays all user accounts. Double-click the user login and type a new password in the 'Password' and 'Confirm Password' fields. Passwords requirements mandate that the password have a minimum of eight alphanumeric characters. The password is also case sensitive.
2. The user's role can also be changed on this screen by clicking the new role.
3. When complete, click Apply and Close to exit.

Modify Roles

A user's role can also be modified.

1. Click the 'User Administration' icon from the main PCC SAT screen. A window will appear that displays all user accounts.
2. Double-click the user who's role needs to be modified.
3. Change the user's role by clicking the new role.
4. When complete, click Apply and Close to exit.

Delete Users

An authorized user has the ability to delete a selected user.

1. From the main PCC SAT screen, select the User Administration icon.

2. Click on the user to be deleted.

3. Select the Delete User icon from the User Administration screen.

A prompt will appear on the screen asking, "You have seletected to delete user 'nnnn' Are you sure?" Click Yes. The user account will be removed from the system and will no longer appear on the User administration screen.

Print User Information

An authorized user has the ability to print the listing of all user information.

1. From the main PCC SAT screen, select the User Administration icon. (Fields can be sorted by clicking on the heading above each column.)

2. Select the print icon from the User Administration screen.

3. A print window will appear which displays all of your printers as well as the default printer that is set up on your system which is indicated with a check mark. Select the correct printer and click Print.

4. The System Users printout will appear on your screen. The 'Ctrl+ arrow' icons at the top of the screen can be used to page forward and backward in the printout (if more than one page). Use Ctrl+Q icon to quit, or to print, click the Printer icon.

Page 1

System Users

Date: 2003-08-07 12:46:32

ALC: 1111111111

Printed By: sharon

Login	User Name	Creation Date	Last Access	Role
admin	System Administrator	2003-08-06 11:41:13	2003-08-06 12:07:02	Administrator
Johnny D	Johnny D	2003-08-06 13:40:13	2003-08-06 14:17:26	Cashier
Sharon	Sharon B	2003-08-06 12:07:27	2003-08-06 14:42:48	POC

Activity Log

The POS software records all action that occur in the POS/SAT. Selecting various settings changes the information that is displayed.

To view the activity log, select the Activity Log icon from the main PCC SAT screen. When viewing the activity log, select the appropriate event types, sources, and modules, or all settings should be checked to capture all system activity. Enter desired date range to view the log.

System Activity Logging consists of several sections:
- Event Types – Types of events logged for viewing.
- Sources – Current sources available
- Modules – Configurable selections. Some examples of these modules are:
  > LAM – Administrator; POS – Point of Sale;
  > LVD – Local Verification database; LID – batch activity
- Date Criteria – User configurable date criteria selection.
- Listing – An event listing of selected sources and/or module by date.
- Trim Log – Clears the activity log based on the SAT system configuration activity log retention setting.
- Print – Ability to print the activity log.

To view information about an event, highlight the desired event. A detailed description of the selected event displays in the Detail section, the ALC+2 displays in the Location section, and the user logged in during the event displays in the User Name section at the bottom of the screen.

The SAT activity log should be printed before an upgrade. It is also recommended that the SAT activity log be printed monthly, or as the agency requires. If your location processes high volumes of checks, a more frequent schedule may be appropriate, because your activity file will be lost if you lose your hard drive. To print the activity log:
1. Select the event types, sources, and modules desired.
2. Enter the date range.
3. Select Print.

Batch Recovery

Authorized users are able to use this feature to recover items from a non-functioning PC to restore items to a backup PC. This would occur when a PCC POS terminal unexpectedly fails prior to batches being transmitted.

Note: The backup or contingency PC must have the same secondary media or a compatible secondary media in order for the batch recovery to work. If the backup or contingency PC is being used to process batches, all batches must be closed and transmitted before using the PC for batch recovery.

If the Secondary Image Storage fails while in the PCC POS application, a batch recovery cannot be performed. Call FRBC at 1-800-624-1373 or 216-579-2112 for assistance or refer to the *Troubleshooting* section of this SOP manual.

To initiate a batch recovery and retrieve the batch from the secondary image storage of the failed PC, do the following on the backup or contingency PC:
1. Close any batch in process and exit out of the PCC POS application.

2. Connect or insert the backup device (PCMCIA card or Zip disk) from the non-functioning PC to the backup PC. If the backup PC is only used as backup hardware, check the following:
   - Date and time are accurate.

- Scanner is connected.
- Printer driver is installed.
- PCC POS application version (refer to *Determining the Version* in this section). If unsure of the correct version, contact FRBC at 1-800-624-1373 or 216-579-2112 for assistance.
3. Launch the PCC SAT application and enter your Login and Password.
4. Select 'File', then 'Configuration' from the menu at the top of the screen. Write down or capture a screen print of the current configuration settings. If these settings need to be altered to accommodate the batch recovery procedure, they will need to be restored once the process is complete (step 18).

Verify the configuration information is the same as the failed PCC information, if unsure call FRBC at 1-800-624-1373 or 216-579-2112 for assistance.
Verify the secondary image storage drive is accurate by selecting the secondary image drive from Windows Explorer (zip drive).
If necessary changes were made, select Apply *to apply the changes, and* Close *to close the System Configuration screen.*

5. Select 'File', then 'Batch Recovery', or select the Batch Recovery Icon from the toolbar.
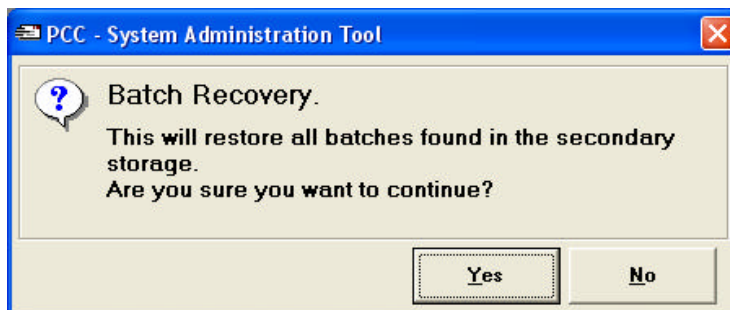
6. Select Yes to accept the batch recovery function.
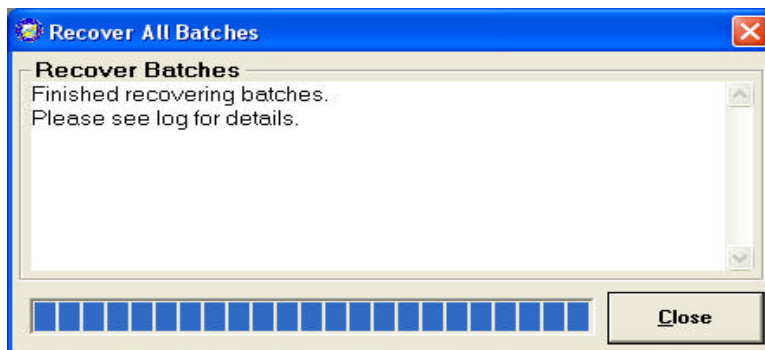
7. Launch the PCC POS application and enter your Login and Password.
8. Select 'File', then 'Configuration' from the menu.

9. The first tab is the Scanner tab. Accept the default Comm Port field (COM1) and Baud Rate (57600). A window screen will appear if the Comm Port is incorrect. Select the correct Comm port (Com1, Com2, etc.).

10. Select the 'Application' tab to change the Terminal ID field, so it matches the non-functioning POS terminal. If unsure of this information contact FRBC at 800-624-1373 or 216-579-2112.

11. Select Apply to apply the changes (if changes are applied), and Close to close the Configuration window screen.

12. Check the SAT activity log to verify the batch recovery was successful. If it was unsuccessful, reseat (remove then replace) the backup device and reselect Batch Recovery or call FRBC at 800-624-1373 or 216-579-2112 for assistance to recover the batch.

13. Once complete, the cashier will then have an active batch list of items that were recovered. Select Close on the Batch Recovery screen. Follow the regular Batch Close process described in the 'Daily Processing' section of this Guide. Balance with item count and dollar amount before you transmit the batch.

14. Once the batch is closed and transmitted, use extreme caution to restore the previous PCC POS terminal configuration to its original configuration prior to further batch processing. Use the information you recorded in step 8 (written or screen print) to restore back to the original configuration if the settings were altered.

Location Verification Database (LVD) Reset – If applicable

If an agency is utilizing the check verification process through the LVD download, there will be occasions where a new LVD is required. Daily LVD downloads contain only new items received by the MVD. If there is a change in the location's policy, or if the POS is re-deployed to a new location, an entire new LVD should be obtained and needs to be requested manually.

To initiate an LVD reset, select the 'LVD Reset' icon from the main PCC SAT screen.

The LVD reset button erases everything on the LVD in anticipation for a replacement with new data. **If the LVD reset is selected and a new LVD is not obtained, there will not be any verification of checks presented.**
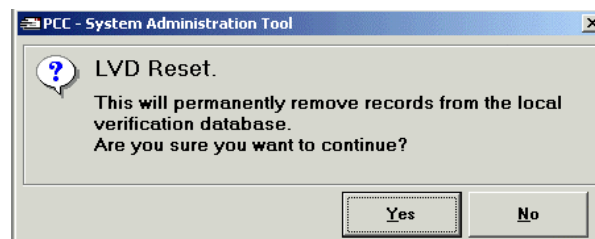
Additional information on the LVD is located in the Master Verification section.

Help

The Help icon from the PCC SAT provides the PCC SAT version information, as well as a link to your computer's system information.
1. Login to the PCC SAT application.
2. Select 'Help', then 'About PCC System Administration Tool'
3. The screen will display the version number for the PCC SAT. This information may be requested from the FRBC or the Treasury for troubleshooting purposes.

POS Application Setup

Signing on to the PCC POS Application

Once an authorized user logs into the POS, the user is presented with the main POS screen. The PCC POS administrator will supply each user with a default password. Initial login requires the user to reset their password, since it was assigned by the administrator. A user's passwords should be known only to that user. After typing the Login and Password, click OK . The user will then be prompted to change their password to one that is known only to that user. The password is case sensitive and must contain a minimum of eight alphanumeric characters.

NOTE: A user must be setup in the PCC SAT application before the user can access the PCC POS application.

POS Configuration

To view or edit current POS configurations, the authorized user will need to go to the 'File' menu and select 'Configuration'.

An authorized user, i.e. an administrator role, has the permission to edit POS settings, including the settings for 'Scanner', 'Application', and 'Reports'.

Scanner Configuration
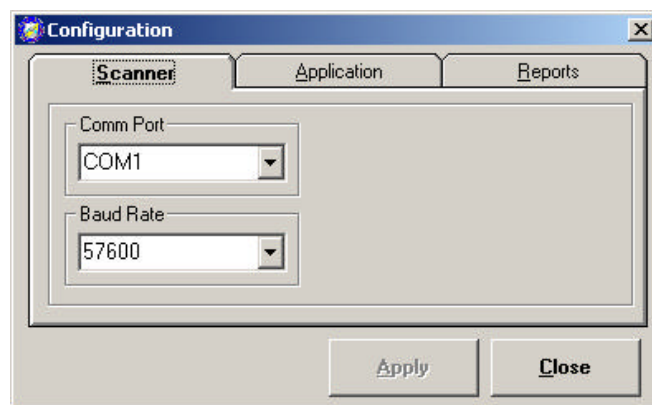
Under scanner configuration a user can change which Comm port is designated for scanner users and can change the transmission baud rate for the specific scanner. The Comm Port and the Baud Rate indicated in the screen above are the recommended settings.

Application Configuration
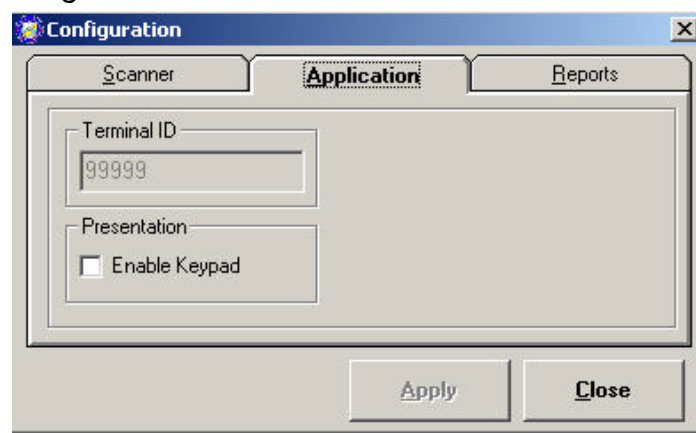
These fields should be confirmed from the initial installation.
- The Terminal ID is provided by FRBC during installation and entered during the Install Shield process. It should not be changed, unless the PC is being used as a backup PC for batch recovery. It cannot be changed from this screen. An authorized user would use the PCC SAT to change the

terminal ID for batch recovery. The Terminal ID on the screen above is only an example. Refer to *Batch Recovery* in *Troubleshooting* section for more information.

- The Enable Keypad should be checked if you are using the Yes/No keypad. The keypad is an optional feature. Enabling the Keypad allows the check writer to confirm the transaction dollar amount. The Keypad feature is disabled while the application operates in the Accounts Receivable/Lockbox mode. Refer to *Requirements and Configuration* earlier in this section for more information on the Yes/No Keypad.

Reports

A printer must be selected/established prior to operation, since it is mandatory to print the batch list as part of the batch closing process.
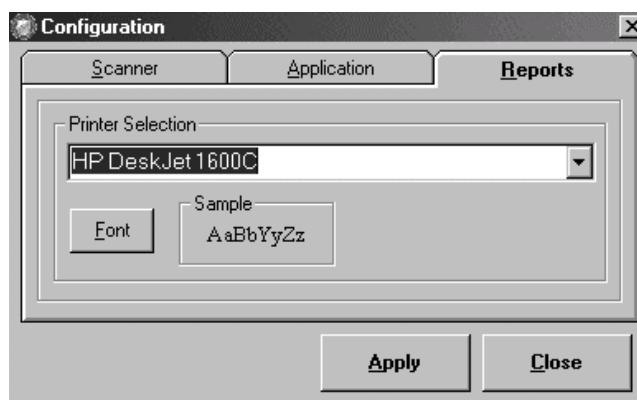
The POS automatically generates a list of printers available based on what printers have been installed on the operating system and/or network. The user can select the appropriate printer used at the location. There must be an established printer to the operating system.

To install a new printer, use the 'Printers' option in the Windows operating system.

Once a printer is installed, a user can select the printer from the drop down menu, under the 'Report' tab within the configuration window.

Users may also select which reporting font is desired on the batch list printouts.

Note: PCC will use the default printer assigned in the operating system if one is not specified on this screen.

Accounts Receivable/Lockbox Mode

Accounts Receivable/Lockbox mode is used for checks that are processed without the customer present during the transaction.

The POS can be configured to operate in Accounts Receivable/Lockbox mode. The application title (top line of screen display) displays followed by "[LOCKBOX]" indicating that the user is in the POS Accounts Receivable/Lockbox setting.

To operate in Accounts Receivable/Lockbox mode, an authorized user must select 'Mode' from the toolbar on the top of the screen, then select 'Lockbox'. 'Lockbox' should be checked indicating you are in Accounts Receivable/Lockbox mode.
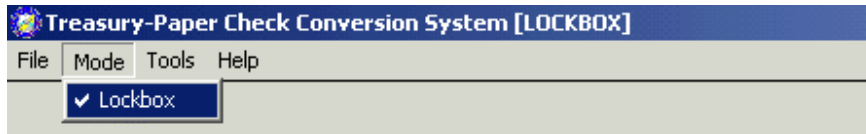
If you do not want to operate in Accounts Receivable/Lockbox, go to 'Mode' and select 'Lockbox' so it is unchecked. A batch must be closed when changing modes of operation. Commingled batches are not permitted. Refer to *Selecting the Processing Mode* in the *Daily Processing* section for more information.

Note: the permission to change modes is limited to those whose role allows them to configure POS.

Updating Check Verification Database, if applicable.

On the PCC POS main screen, choose 'Tools', then 'Update the Check Verification Database'. The PCC POS utilizes the check verification database to obtain identified closed and blocked accounts to prevent acceptance of these checks drawn on these accounts. The Update Check Verification Database option can be used to obtain more frequent updates of closed and blocked accounts since the last batch transmission, as well as to obtain a complete download of closed and blocked accounts when a PCC POS is installed or re-installed.

Authorized users can update the LVD by selecting 'Tools' from the menu on the top of the POS screen, then selecting 'Update Check Verification Database'. Only certain authorized users have the ability to request LVD updates.
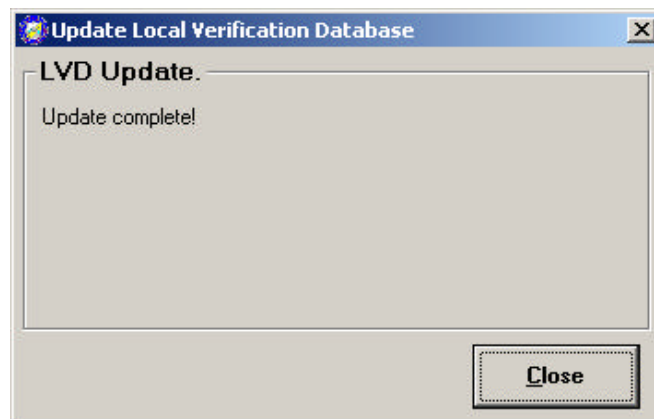
About the POS

Help

The 'Help' menu supplies information about the PCC POS software and scanner version as well as a link to your computer's system information. Select 'Help' from the toolbar on the top of the PCC POS main screen, then select 'About PCC POS'.
1. Login to the PCC POS application.
2. Select 'Help', and 'About PCC POS'.

The screen will display the version number for the PCC POS. This information may be requested from the FRBC or the Treasury for troubleshooting purposes.
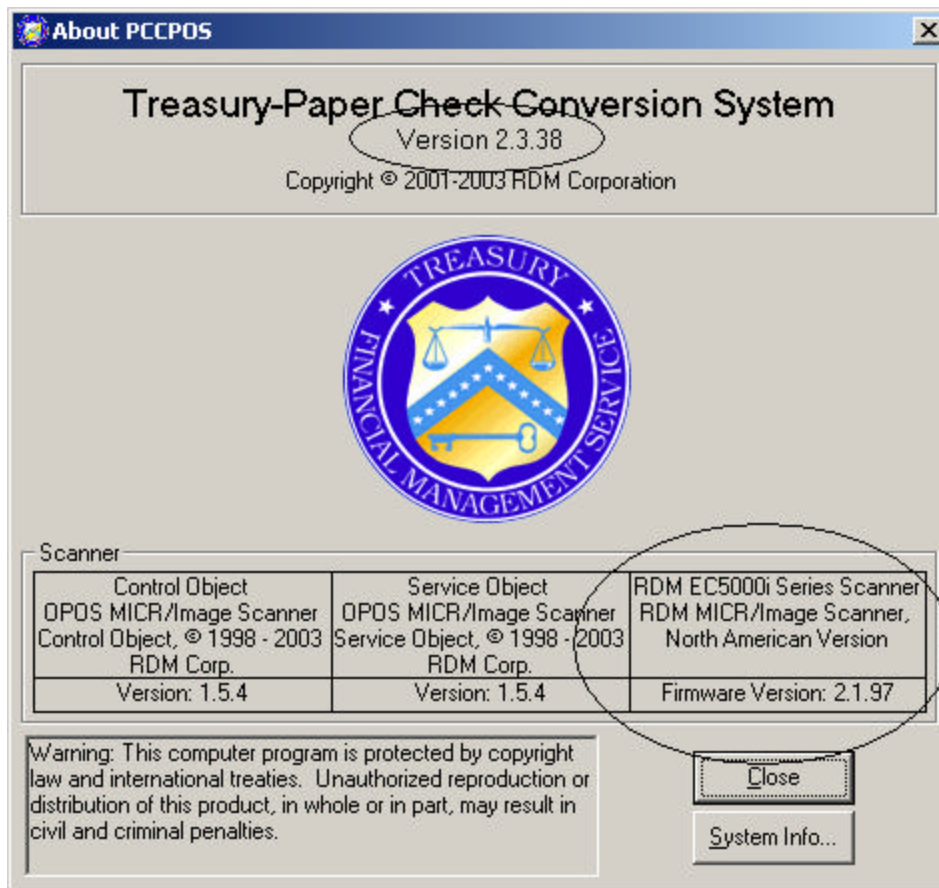
United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Daily Processing

Revised October 8, 2003

Table of Contents

Daily Processing
Step-By-Step User Guide

Access Login

After successful installation and configuration, user can double click the PCC POS desktop icon

to start the application.

The user will be prompted to enter their 'Login' and 'Password'.

NOTE: Users will be given a 'login' and an initial 'password' by an authorized user of the SAT application. Upon initial login, they will be required to change the password.

After the login and password have been entered, select OK or press 'Enter'.
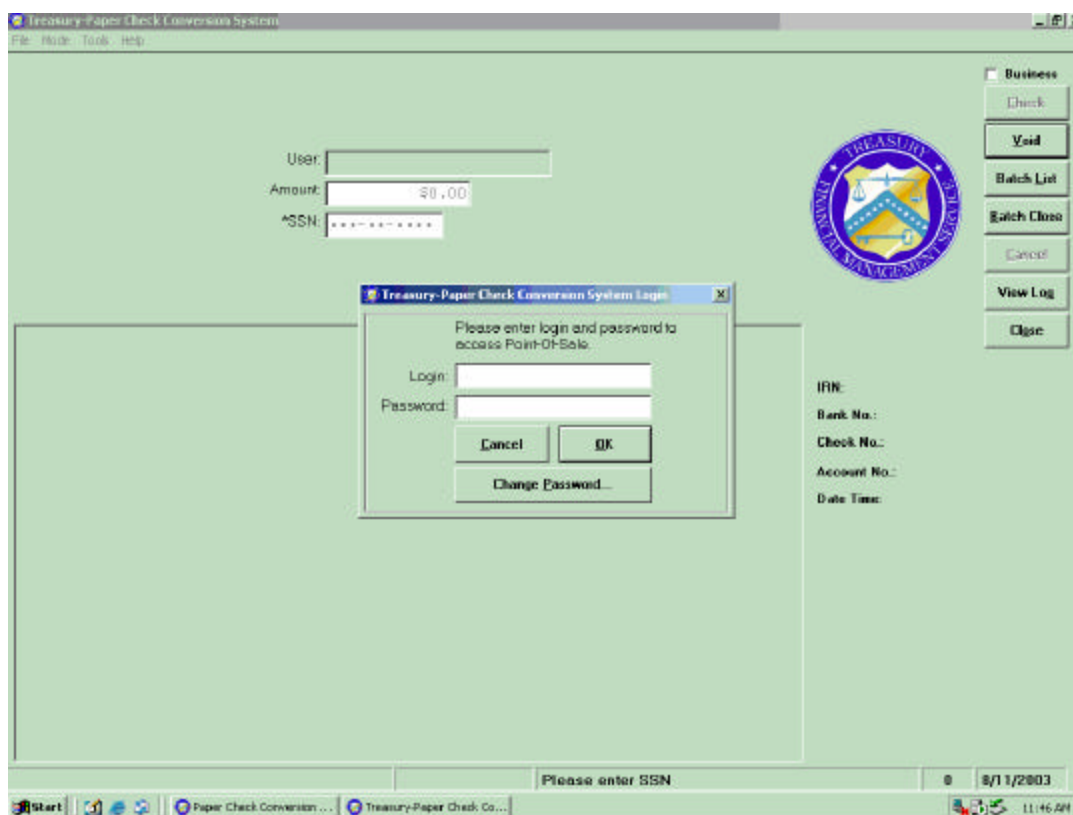
The Main POS window is configured depending on the respective agency's requirements. In addition to the user and amount field, an agency may configure the POS window with up to four fields. Fields proceeded by an asterisk (*) require mandatory input.

NOTE: The user will remain active in this session until the batch is closed or the user logs out, or if the PC is configured to shutdown automatically after idle for a certain period of time. Also, the user is linked to all items scanned and all activities attempted, both successful and unsuccessful. All activities are logged by the user in the activity log and are retained for a specified number of days configurable by the agency.

For agencies utilizing the Check Verification Database, the user may be prompted to update the Check Verification database upon login. If the Check Verification database has not been updated within the agency's requirements (as determined in the SAT configuration setting), the user is prompted to update the database. This could occur if the user was unable to connect to the Internet or remote location for an extended period of time.

NOTE: Mobile/remote users should update the Check Verification Database prior to mobilization by selecting 'Update Check Verification Database' from the Tools menu on the main POS screen.

The Check Verification Database update occurs automatically at batch close, so selecting 'Yes' at this prompt is optional. This will modify your LVD records before processing your activity for this batch.
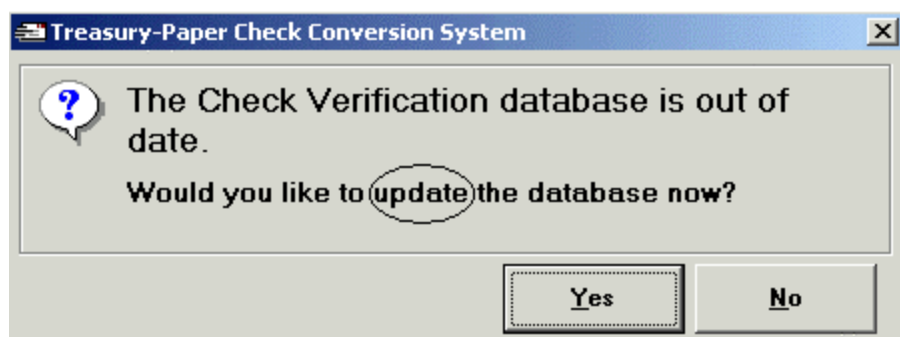
If you select Yes, the database will be updated. If you select No, the existing check verification information will be used when processing check data and the following message will be displayed:

If you select Yes , an authorized user with permissions to override an update is required to approve the action by entering their login and password. If No is selected, you will receive an error message indicating that the POS application is not ready and checks cannot be processed. To determine the authorized user refer to *Configure System Roles* in the *Installation and Configuration* section.

Select the Processing Mode (POS or Accounts Receivable/Lockbox)

The Paper Check Conversion system is able to process checks either through standard Point of Sale (POS) mode - where an individual is cashing a check or purchasing a good or service in person, or through Accounts Receivable/Lockbox mode. Accounts Receivable/Lockbox mode is used when the writer of the check is not present, i.e. when checks are received through the mail as payments.

Not all agencies will utilize both the Accounts Receivable/Lockbox and POS mode. Furthermore, your site may choose not to use both modes everyday, due to fluctuation in check volume.

The processing mode, either Accounts Receivable/Lockbox or POS, is established by an authorized user by selecting 'Mode', then 'Lockbox' from the toolbar on the top of the POS main window. If Lockbox is checked the application is in Accounts Receivable/Lockbox mode as indicated on the application title bar. The screen below shows the application operating in Accounts Receivable/Lockbox mode.

Application title bar indicates Lockbox mode.
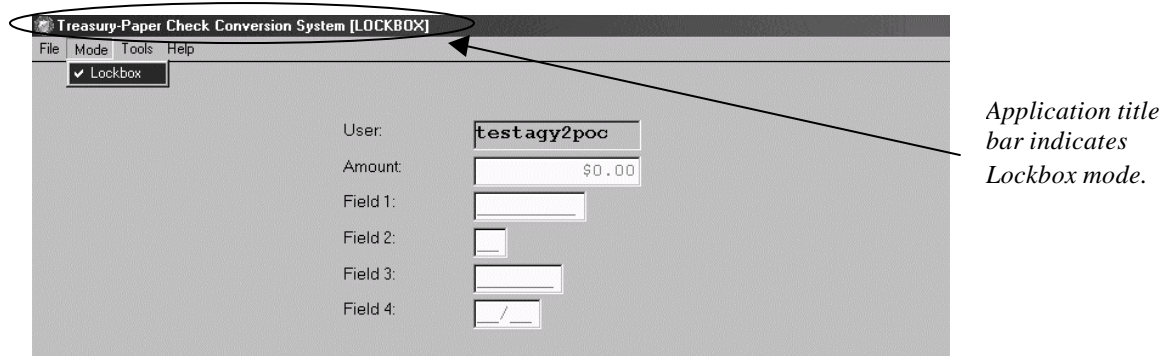
The processing mode can be switched throughout the day, but the POS application requires that any checks processed prior to the change in processing mode be closed in a batch and transmitted to the CIRA. **A batch can only include one type of processing mode. POS and Accounts Receivable/Lockbox checks cannot be commingled.**

Type of Check – Business or Personal

The POS application can process both personal and business checks in a single batch. The cashier should inquire if the check is either a personal or business check. While most business checks are typically larger in size, business checks can look the same as personal checks. The account owner should be your determining factor to decide if the check should be classified as personal or business.

If the check is a business check, the operator must select the 'Business' box located above the Check button on the main POS screen. The operator must scan the front and back of business checks and all checks processed in the Accounts Receivable/Lockbox mode.
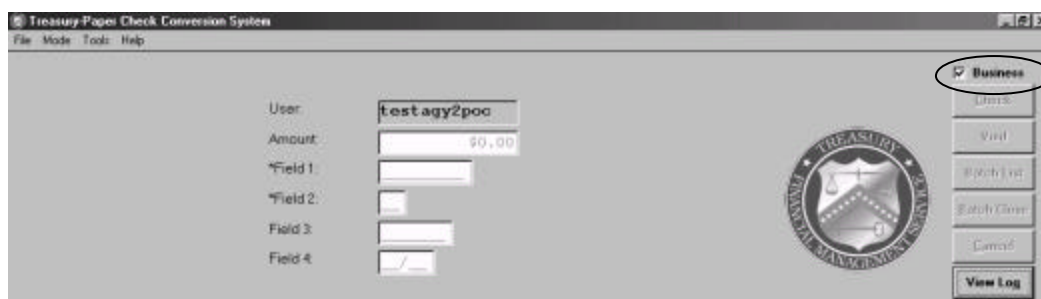
NOTE: Upon selecting the business check box, the POS application will continue to process checks as business checks until the box is unchecked. The operator should establish the status of each check and select the appropriate check type.

If a business check was detected, due to the format of the MICR line, but the business check box was not selected on the POS screen prior to the scan, the following message appears:
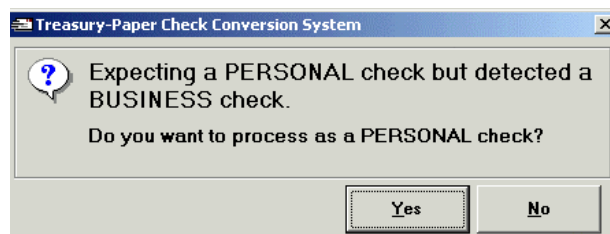
Select No if a business check is being processed, or Yes if you are processing a personal check.

A similar message appears if processing in business check mode, but a personal check was detected.

Process a Check

Checks that should not be processed through PCC

The following types of checks should NOT be processed through PCC:

- DO NOT accept checks that do not have a check number. These checks cannot be processed due to Treasury and NACHA (National Automated Clearing House Association) rules. An example could be temporary checks issued for new checking account customers.
- US Treasury Checks
- Third-party checks
- Credit card checks
- Obligations of a financial institution, including but not limited to traveler's checks, cashier's checks, official checks, or money orders
- Checks that state "DO NOT ACH", "NOT FOR ACH/EFT USE", or words to that effect
- Checks drawn on state or local government including state warrants
- Checks payable in a medium other than the United States currency
- Checks drawn on foreign (non-U.S. financial institution) checking accounts
- Payroll checks

NOTE: The above items may be processed through the same paper channels you used prior to PCC.

NOTE: Apply any necessary stamps in a location that does not interfere with the dollar amount or the signature. Since you will not be depositing PCC items at your bank, there is no need to stamp "For Deposit Only" on the back of the check.

Scanning a Check

For business checks and checks processed in Accounts Receivable/Lockbox mode, the operator will be alerted to scan both the front and back of the check.

The bottom of the PCC POS screen will display, 'Please press enter to begin'. Once the 'Enter' key is pressed, the scanner light will turn green, indicating that the scanner is ready to accept a check/coupon. The bottom of the PCC POS screen will then display 'Scan front of Check'.
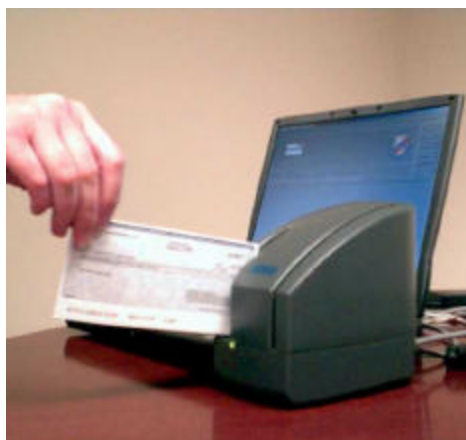
1. A single beep will sound indicating a check has been scanned successfully.

NOTE: If a triple beep occurs, cancel and process check again.

Scanner Light Color	Indicates
GREEN	Scanner is ready to accept a check and capture its image
AMBER	Scanner is in standby mode, not ready to accept a check
BLINKING RED	Unable to read check image. Cancel and try again, possibly with another check. Make sure that the check is inserted correctly.
CONSTANT RED	There is a problem with the scanner. Cancel the transaction and retry. See section in Troubleshooting.

NOTE: For more detailed information regarding the scanner, such as scanner ports, scanning checks, cleaning the scanner, etc., refer to the RDM scanner documentation in the Appendix.

2. The application will show a status bar on the bottom of the POS screen indicating the capture of the image. Once the capture is complete, the image will appear on the screen.

3. Ensure that the entire check image is visible on the screen and the dollar amount must be legible. (A check may successfully scan even though the item was folded going into the device.) If the image is not legible, click 'Cancel' and re-scan the check.

4. If this is a business check or the PCC POS is in the Lockbox mode, the bottom of the screen will display, 'Scan back of check'.

5. After the check has been scanned, the cursor will be active on the 'Check Amount' field. Enter in the amount as found on the image displayed in the lower portion of the screen and press Enter.

NOTE: Only numbers need input. For example, entering in 1290 would equal $12.90, and 56321 would be equal to $563.21.

NOTE: Be sure to verify the check dollar amount input into the POS to the actual check. If an incorrect amount is entered and the customer has left, there is no way to alter the amount of the check and it cannot be voided and reentered since the check is not available to scan again. To correct prior to closing the batch, have the customer come back, void the incorrect item in the POS, and process the correct transaction. If the batch has already been closed, notify the Federal Reserve Bank of Cleveland to help in resolving the problem. Refer to the Troubleshooting section for more information.

NOTE: The PCC POS application does not utilize the mouse and touchpad. When entering information into the data entry fields, use only the ENTER key to move from field to field. Using the mouse and/or touchpad can lead to data entry errors.

Enter the information in the agency specific fields, then press 'Enter'. All fields which contain an asterisk (*) are required agency specific fields configured for a specific character or numeric value. The transaction will not be completed if these fields are left blank. The operator should complete all fields using information submitted with the check, i.e. bill, form number, period being paid, etc. to facilitate the agency's internal processing.

6. Once all the configurable field information is entered, please verify that the Check Amount and configurable field information are correct, prior to pressing Enter to process the transaction.

7. Select 'Enter'. The check is processed and the following additional information displays:
   - IRN (Unique Transaction ID)
   - Bank Number
   - Check Number
   - Account Number
   - Date-Time

8. Select 'Enter'. The transaction is now complete. After 15-30 seconds the screen will clear for the next check.

9. Select the Check button or press 'Enter' to go to processing the next check immediately.

10. Each check that is processed must be stamped with 'VOID – Electronically Processed' after the transaction is complete and the check has been scanned. Checks must be given back to the person with their cash if processed in person. If processed in the Accounts Receivable/Lockbox mode, checks must be destroyed within14 days, according to the Agency Participation Agreement and rules governing lockbox.

Using the Yes/No Keypad

(See Installation and Configuration for instructions on activating/deactivating the Yes/No Keypad)

For agency's using the optional Yes/No Keypad, the customer will be requested to verify the dollar amount using the Yes/No keypad. After the check is scanned and check information is entered, the application bar on the bottom of the POS screen will indicate that customer validation is needed.
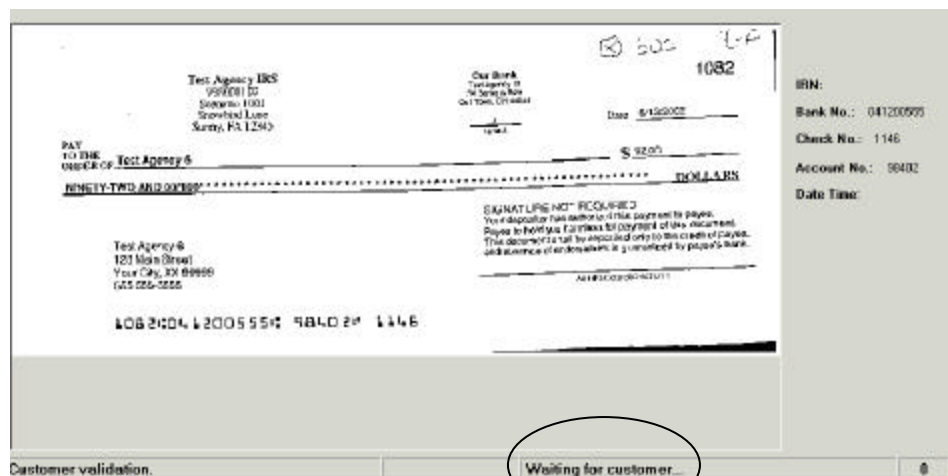
If the customer does not validate the transaction using the Yes/No Keypad after a short period of time, the following message appears:
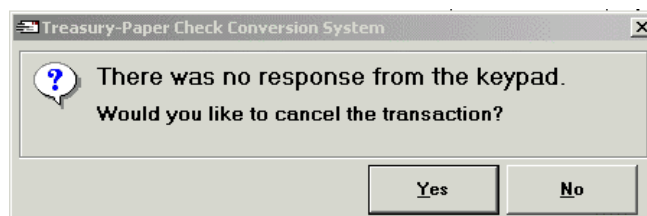
Select No to proceed, and give the customer more time to take action, or Yes to cancel the transaction.

On the Keypad, the customer should press the 'green' key to approve the amount or the 'red' key to decline the amount. The Yes/No Keypad is not available while in Accounts Receivable/Lockbox mode since the customer is not present to approve the transaction amount.

If the customer approves the transaction by pressing the 'green' key, the following message appears. Select OK. The transaction is complete, then the screen clears for the next check.
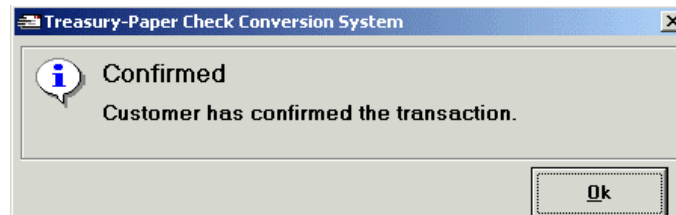
If the customer declines the transaction by pressing the 'red' key, the following message appears. Select OK. The transaction will be cancelled, then the screen clears for the next check.
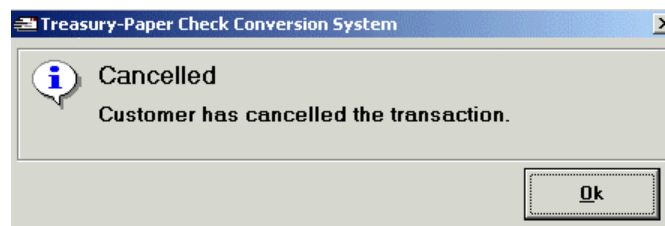
Check Verification Process

Blocked Item

If the agency and or location utilizes the check verification database, the cashier will receive notification if there is a problem on the account or with the agency's specified verification field. If the presented check is drawn on an account or verification field that has been identified as a red flag, the cashier will receive the following message:

An authorized person at the location can override a blocked message by selecting Override.
(Note: When an override of a blocked item is performed in the POS, the override is a temporary,

one-time event. The item will remain block in the MVD unless an authorized person clears the item if the MVD). The authorized person can access the MVD as discussed in the *MVD* section to research the history of the related account. If you are not an authorized user, the following message will appear.
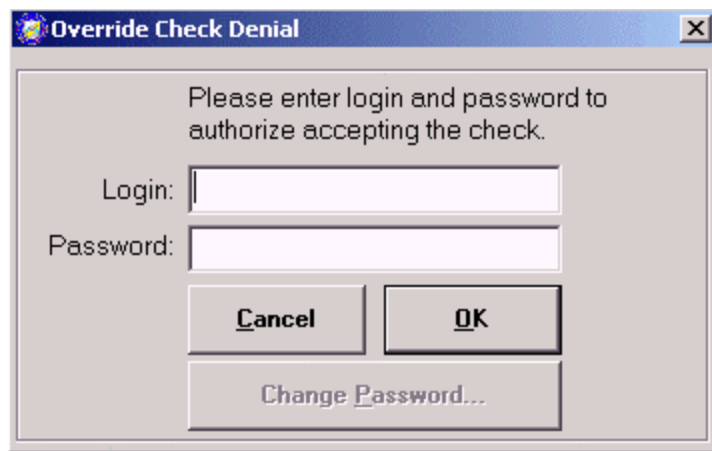
As part of the override process, the approving party will need to add a comment as to why the check was approved for processing.
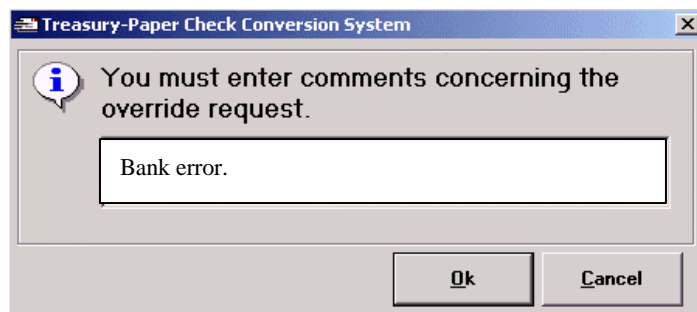
The authorized person then receives a message that the blocked check was successfully overridden as shown below.
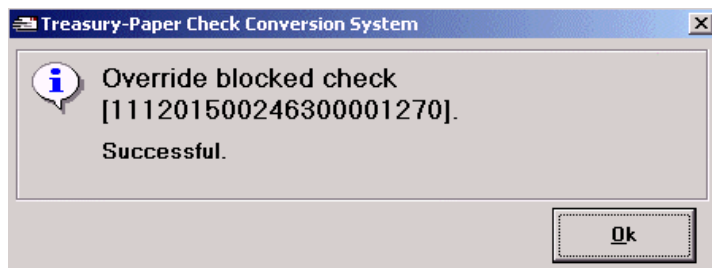
Suspend Item

If the agency and or location utilize the check verification database, the cashier will receive notification if there has been negative return(s) received previously on either the account or the agency's specified verification field. Based upon the location's policy, the number of returns will

impact the suspension period. If the presented check is drawn on an account or verification field that has negative return items, the cashier will receive the following message:
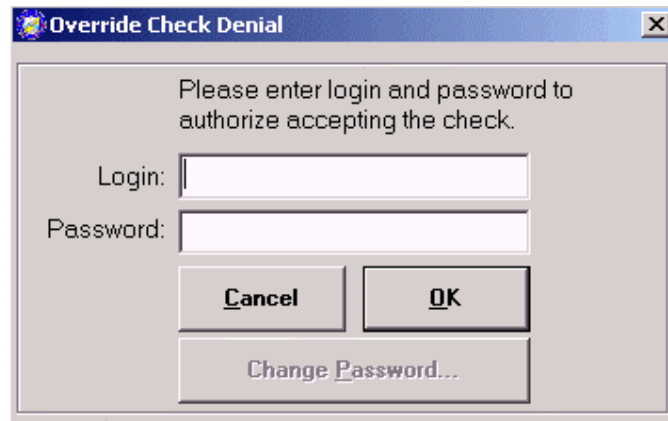
To determine where the return file originated, the cashier or person with the return will require assistance from an authorized user who has researching access to the MVD (i.e. research the site where the return originated).

An authorized person at the location can override a suspend message by selecting Override. The authorized person can access the MVD as discussed in *MVD* section to research the history of the related account. If you are not an authorized user, the following message will appear.

As part of the override process the approving party will need to add a comment as to why the check was approved for processing.

The authorized person then receives a message that the blocked check was successfully overridden.

Deny Item

If the agency or location utilizes the check verification database, the cashier will receive notification if the number of allowable negative returns has been exceeded or if a negative return on a closed account has been received. Based upon the location's policy, the number of allowable negative returns will impact how rapidly an account moves to a deny status. If the presented check is drawn on an account or verification field that has exceeded the allowable negative return policy, the cashier will receive the following message:
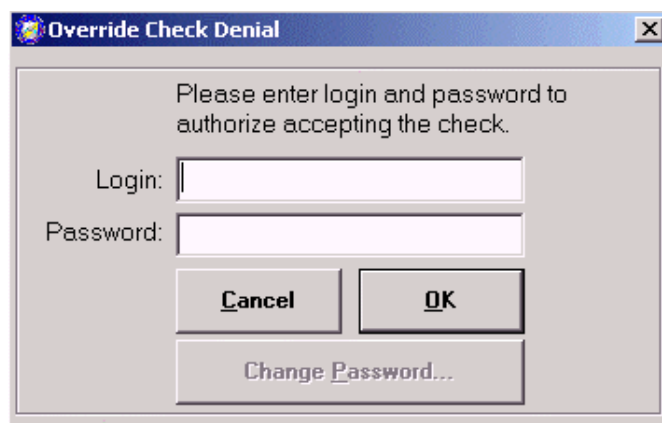
An authorized person at the location can override the deny message, except for instances where the account has been closed, by selecting Override. The authorized person can access the MVD as discussed in *MVD* section to research the history of the related account. An account is tracked by the agency's first required configurable field.

If you are not an authorized user, the following message will appear.

As part of the override process the approving party will need to add a comment as to why the check was approved for processing.

The authorized person then receives a message that the blocked check was successfully overridden.

How to Cancel a Check

While processing a check, prior to pressing Enter after inputting the configurable fields, it is possible to cancel a transaction by selecting Cancel .

If the check has already been assigned a transaction number as found in the bottom of the screen, it has been entered into a batch, and can no longer be cancelled. Please refer to *How to Void a Check*.

How to Void a Check

ONLY TRANSACTIONS THAT HAVE BEEN COMPLETED AND HAVE NOT BEEN TRANSMITTED CAN BE VOIDED.

Transactions may need to be voided for various reasons. Once checks have been entered into the application and the batch has not been closed, a user may find the need to void a check. This may occur if an item is duplicated or if the check writer requests that a previously entered check not be processed.

The void feature can be initiated by the operator; however, supervisory users will need to approve or complete the transaction with a description on why the item was voided.

To void a check:
1. In order to void the completed transaction, the check writer must provide the cashier with the physical check that was scanned. Any item that is voided must be printed first. Refer to *Viewing and Printing Checks*. The printed check must be given to the supervisory user for a signature **prior** to voiding the item.
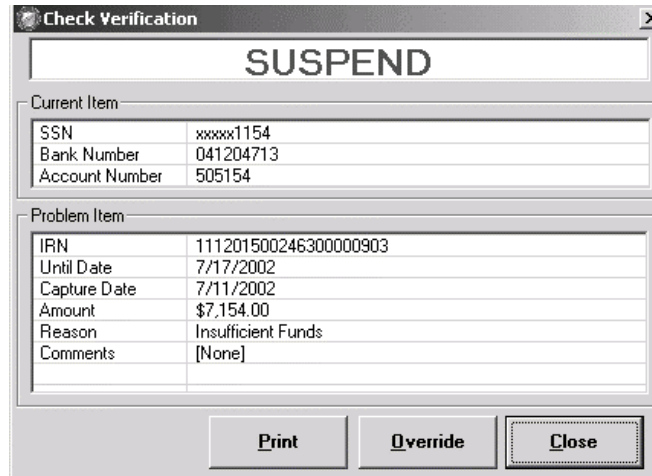2. Once the check image is printed and signed by the supervisory user, select Void from the main POS screen. A 'Void Check' window will appear with a list of checks that have been entered. Items that have not been transmitted will appear on the screen.
3. The operator will select or click on the check that needs to be voided.
4. If funds have already been given to a customer, the funds must be returned to the cashier when a check is voided. The cashier must stamp or write on the physical check with 'VOID: Non-negotiated item'. The cashier can return the check to the person.
5. Once the check has been selected, the user must click on Void .
6. A confirmation window will appear asking you 'Are you sure?'
7. If you select 'Yes', an authorized user's login and password may be required to approve the void. The authorized user will be prompted to enter comments regarding the void request.
8. A confirmation window appears stating the 'Void' process was successful. Once the item is voided it will remain both in the void and batch list marked with a status 'Void'.

9. If you select 'No', the window closes and returns you to the 'Void Check' batch list.
10. Once you have finished, select Done. This will close the Void window and the Main Window
    becomes active again.

Voiding a check results in an event noted in the activity log, indicating that a particular check has been
voided. Voided items are not transmitted to the Central Image and Retrieval Archive (CIRA) for long-
term storage. Only approved items are transmitted.

How to View & Print a Batch List

A Batch List is the list of all transactions that have been processed by the POS, but not yet sent on to CIRA for further processing. The Batch Close process collects the information for all transactions and transmits them to the CIRA for further processing. The batch list must be printed during the batch close process.

To view a current 'Batch List' you must select Batch List on the Main POS Window. This window allows a user to scroll through and view each item. An authorized user may view the batch list at any time during an open session.

The batch list can be sorted according to specific column data, by double clicking the preferred column heading.

The summary box to the right of the check image indicates the following:
  Approved – Successful check transaction
  Void – Voided checks
  Total – Total 'approved' amount

Users are presented with the ability to print the selected check or the entire list of all items in the batch. To print the Batch List, select Print List from the Batch List window.

A preview window will appear in which you can view, zoom, page scroll, and print the Batch List.
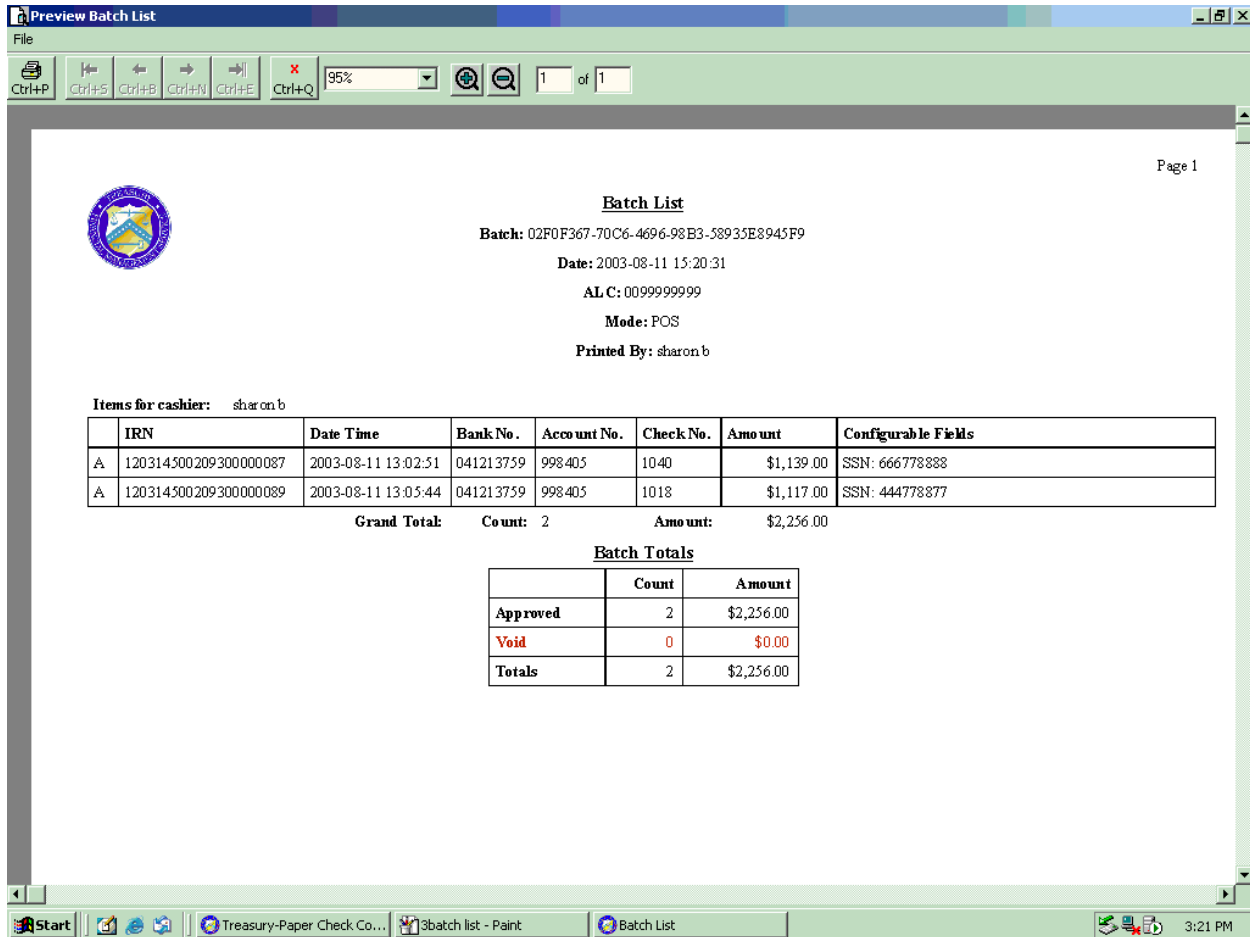
NOTE: The Batch List header only appears on the first page of the printout.

Batches can consist of more than one cashier or POS operator, but not of more than one processing mode. If a batch includes checks processed by more than one cashier, each cashier's items will appear on separate pages with that cashier subtotal count and dollar amount. A total count and dollar amount for all cashiers appears on the last page of batch list.

To print the 'Batch List', select the printer icon at the top left corner. Once complete, the application returns to the 'Batch List' window.

Select Done when you are finished.

Refer to *Appendix A – Sample Reports,* for more information on Batch List.

How to View & Print Checks

Should there be any question on a certain check that has not yet been sent to the archive, the cashier is able to view and print the image of a check from the POS application batch list. Check images are available online from the CIRA web site after the batch is closed by authorized personnel. See the *CIRA* section for instructions.

To view checks in the current batch (that has not yet been closed) , select the Batch List on the Main POS Window. This option presents a window to scroll through and view each check.

To print a check, select the check to be printed, then select Print Check.

A preview window will appear, providing the ability to view, zoom, page scroll, and print the check and check information.
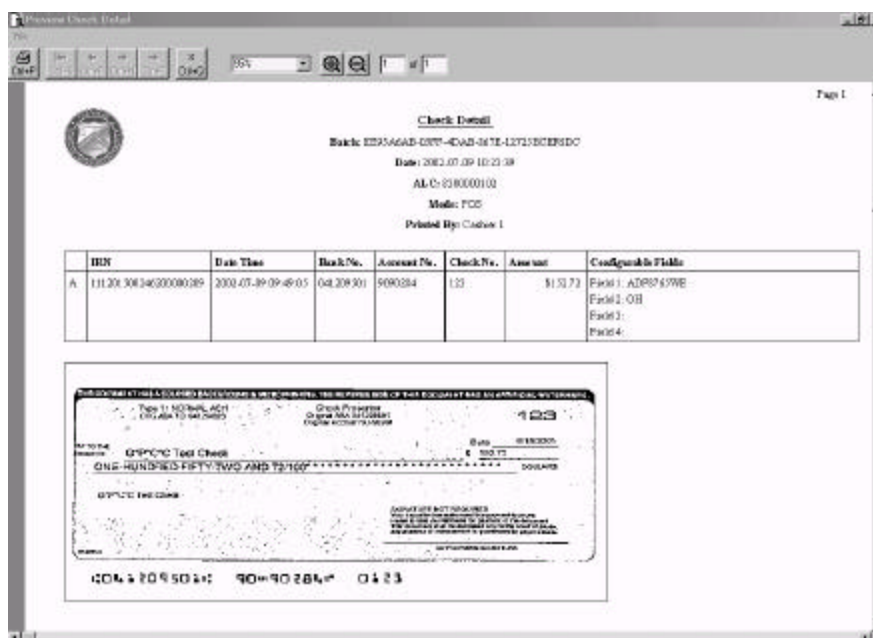
To print the check, select the printer icon at the top left corner. Once this process is complete, the 'Batch List' window will reappear on the screen.

Select Done when finished.

Batch Close

CASHIER MUST BALANCE BEFORE CLOSING A BATCH. Balance to the list of transactions accepted for the day or since the last time the batch was closed.

The Batch Close process must be performed when the processing mode is changed, and at either the end of a day, shift, or when a location desires. Cashiers must balance their activity using the batch list before

closing and transmitting their batch. Refer to the *Troubleshooting* section if the batch is transmitted out of balance.

Select Batch Close from Main Window.

Closing a batch will transmit checks to the CIRA site for archive and to begin the electronic processing. Only items that properly reflect processed transactions should be transmitted to the CIRA.

You are presented with a 'Batch List' window and two options: Close Batch, and Done.

Selecting Done will close the current window and no action is taken.

If Close Batch is selected, a confirmation window will appear showing the number of items in the batch and a question stating 'Are you sure?'
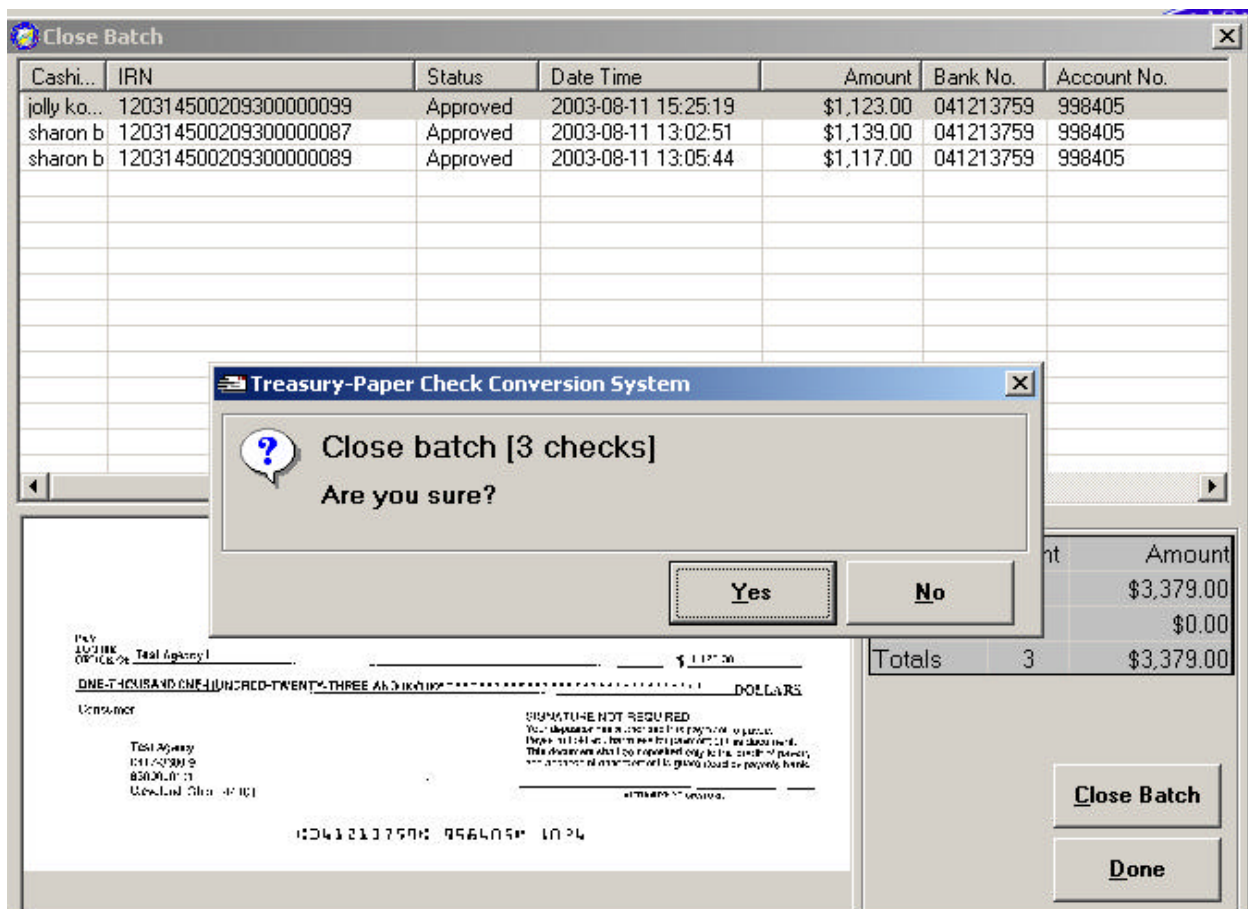
Selecting No will bring you back to the previous window.

Selecting Yes will then display the print window, where the user must click on the printer icon to print the batch list.

NOTE: The batch list contains approved and voided items.

Selecting the printer icon will start the secure transmission process. Confirm that the Batch List was printed by selecting Yes or No.
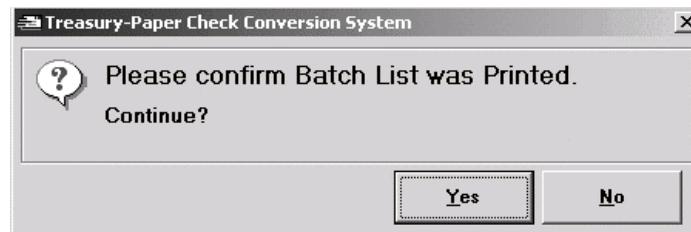
NOTE: The batch will not close unless the user acknowledges that the batch is printed. If the user responds with Yes even if the batch did not print, the batch will close and there will not be a printed record of the batch. If the user experiences difficulty in closing the batch, please refer to the Troubleshooting section.

NOTE: Any checks processed after an unsuccessful 'Batch Close' will be added to the current batch until the Batch Close process is successfully completed.

The batch begins transmitting/archiving to the CIRA. On successful completion the batch list will be deleted and you will have to select Close. A message may then appear indicating the activity log was successfully cleaned. Select Close.

If the agency utilizes the Check Verification Database, the LVD is automatically updated during the batch close. Once a batch has been closed successfully, the current session ends and the application will delete expired LVD records and new LVD records are received. Select Close.

At this point the user will be prompted to login to the POS to begin a new session, or cancel to exit the POS. The Login window appears automatically.

If batch transmission was unsuccessful then the 'Batch List' will be saved on the POS. The inability to close a batch may be due to a variety of reasons, including connectivity problems. If an error message is received, print or note the error message. The error message will also display on the activity log. Select Done. At the next login, a message will appear indicating that the "Batch has not been transmitted". Select Yes to transmit the batch to the CIRA, if you have connectivity. Select NO if the batch should not be transmitted to the CIRA.

NOTE: Currently, anything received before 9:30 p.m. EST will be reflected on the next day's deposit SF215.

Batches should be closed and transmitted on the same business day the activity occurred.

NOTE: If any error messages are obtained during any of the batch close process, the error message (and detail if available) should be copied for troubleshooting and incident reporting

POS System Activity Log

The activity log is a listing of all actions, including transactions performed on the POS application. The log reflects all logons, log offs, checks processed with their unique ID, annotates voided and cancelled checks. The activity log will also show when a batch has been successfully closed. A sample activity log is found in *Appendix A*. An authorized user may view the log at any time.

Select View Log from the main POS screen. When viewing the activity log, select the appropriate event types and modules, or all settings should be checked to capture all system activity. Enter the desired date range to view the log.

Similar to the SAT log, the POS log consists of Event types, Modules, Location, and Username.

A listing of events and the detail for each event is available according to the date selection.

A user may also print this log for various reasons. The activity log should be printed prior to new installation and on a monthly basis or as required by the agency.
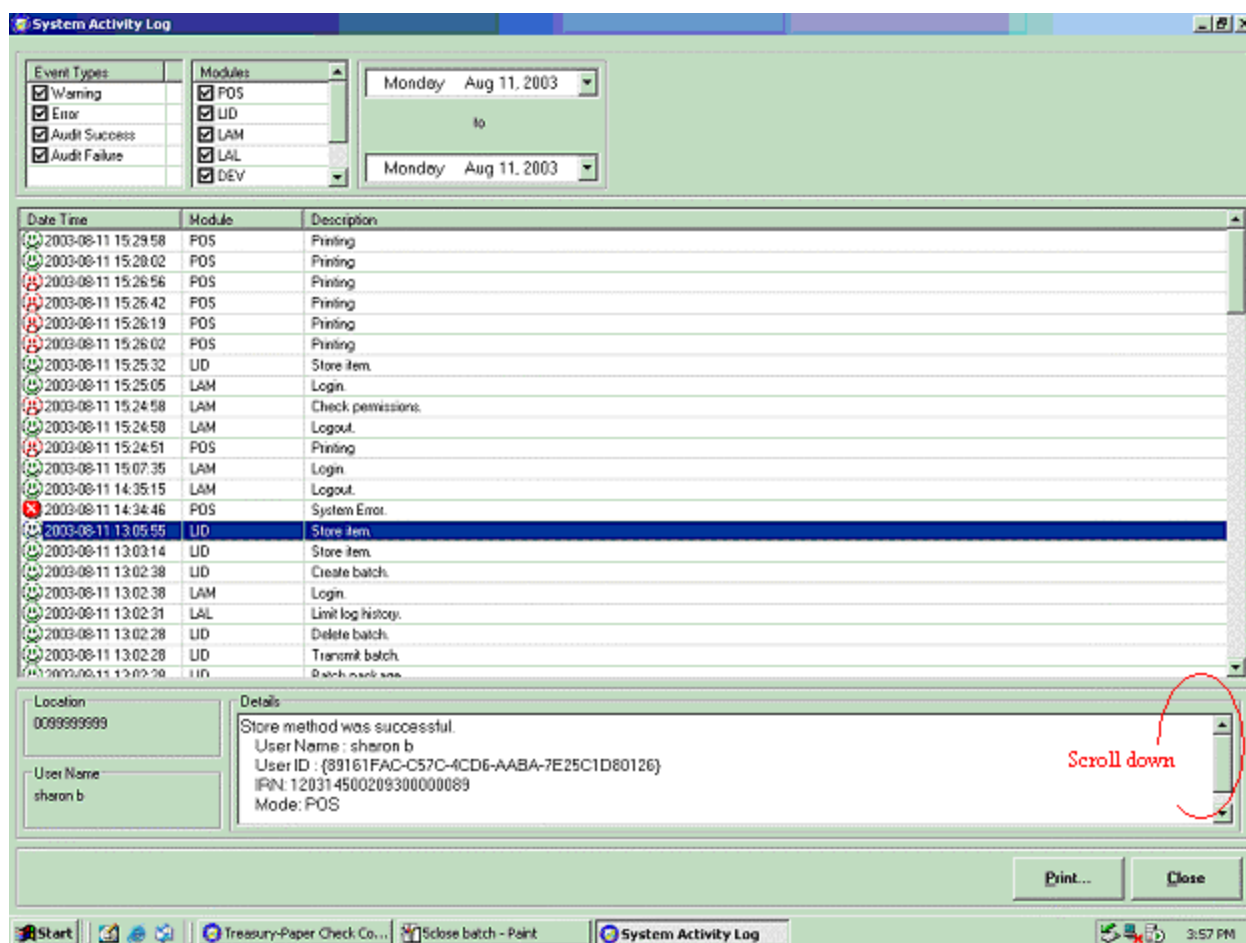
POS System Activity Logging consists of several sections:

- Event Types – Types of events logged for viewing.
- Modules – Configurable selections.
  > LAM – administrator; POS – Point of Sale;
  > FTX – file transfer from POS to CIRA; LID – batch activity
- Date Criteria – User configurable date criteria selection.
- Listing – An event listing of selected modules by date.
- Print – Ability to print the activity log.

To view information about an event, highlight the desired event. A detailed description of the selected event displays in the Detail section (scroll down), the ALC+2 displays in the Location section, and the user logged in during the event displays in the User Name section at the bottom of the screen.

The log should be printed prior to a new installation. It is also recommended that the log be printed periodically each month. To print the activity log:

1. Select the event types and modules desired.
2. Enter the date range.
3. Select Print.

Logging out of the POS Application

To log out of the application, select 'File' from the menu at the top of the main POS screen.

Select 'logout'. The logon box appears. This enables another user to logon without exiting the application completely. If a cashier logs out of the application without closing a batch, the cashier will be reminded that the batch is still open. To logout completely, select Yes to the prompt, 'Logout Point-of-Sale'?
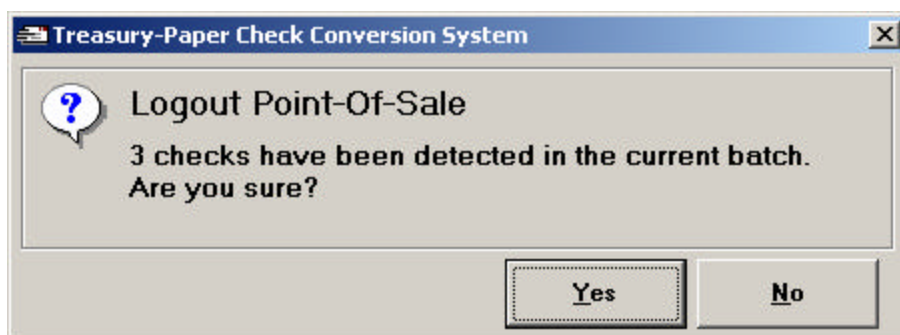
Exiting the POS Application

To exit the application:

Select 'File' from the menu at the top of the screen.

1. Select Exit. A confirmation window will appear.

2. Selecting Yes will exit the application and return the user to the Desktop.

3. Selecting No will return the user to the previous screen.

If a cashier exits the application without closing a batch, the cashier will be reminded that the batch is still open. Selecting Yes will allow the cashier to exit anyway. Selecting No will allow the cashier to stay within the application in order to transmit the batch.
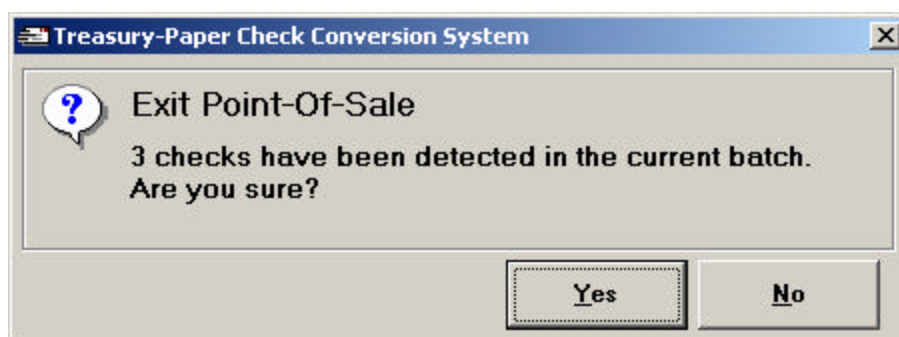
The application can also be exited by clicking the 'close' button, X̄ at the upper right of the screen. A confirmation window will appear prompting, 'Exit Point-Of-Sale'.

1. Selecting Yes will exit the application and return the user to the Desktop.

2. Selecting No will return the user to the previous screen.

If the cashier chooses to exit without transmitting a batch, the next cashier that signs on will be prompted whether or not to continue with the batch. If the operator or cashier selects Yes, the POS will allow the cashier to add additional items to this batch. If the cashier or operator selects No, the operator will be prompted to close the batch. Select Ok to start the close batch/transmission process or select Cancel.

NOTE: Voided items are counted as batch items.

If NO is selected, the Close Batch window appears, enabling the operator or cashier to close the batch before processing additional checks.

United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Master Verification Database (MVD) & Central Image Research Archive (CIRA)

Revised October 8, 2003

Table of Contents

Master Verification Database (MVD) & Central Image Research Archive (CIRA)

What is the Master Verification Database?

The Master Verification Database (MVD) is a central component of the Verification system. It provides the Point Of Sale (POS) system information to ensure a presented check is acceptable. The MVD is a "negative" database containing "return" information on checks and accounts that have failed to clear in a previous PCC transaction attempt, and "blocked" accounts/routing numbers or individuals that have been identified where future transactions are not desired. The essence of this service is to advise the POS operator that the presented item has had a prior transaction returned. This information can be used to determine whether or not the transaction should be completed on the POS equipment. The following diagram offers a high level view of the entire system.
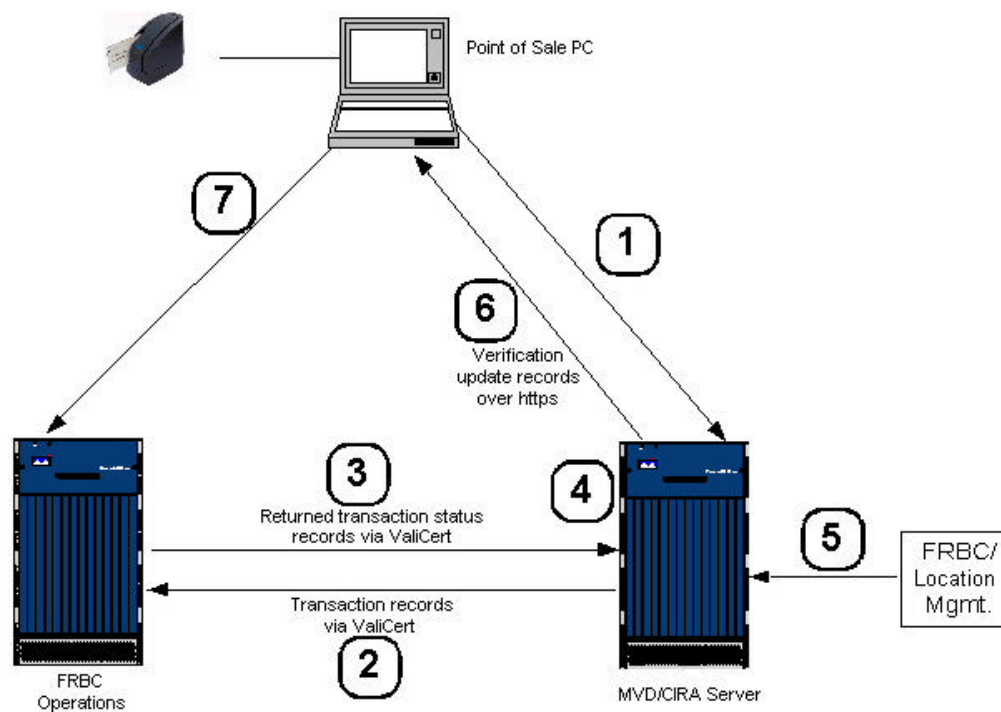
1. Check transactions are processed at the point-of-sale and sent to the MVD/CIRA.
2. Check transaction data is sent from the MVD/CIRA to the FRBC operations
3. The negative returns on check transactions are sent from the FRBC operations to the MVD/CIRA.
4. Verification record is completed with information from original payment transaction.
5. FRBC or Location Management submits blocked records to the Verification Server.
6. Periodically, the POS System requests an update from the Verification Server to keep the POS System's local verification database up-to-date.
7. When subsequent checks are processed at the point-of-sale, the routing number/account and the agency's required configurable field (SSN, drivers license, etc.) information is validated against the verification database.

How Does the MVD Work?

Verification records originate from returns of previous processed payments originated through the PCC system, as well as manually entered records (i.e. block record). A subset of the MVD, based on requesting location and defined configurable filter parameters, is forwarded to the local field POS application. This subset is known as the Local Verification Database (LVD). Blocked data is entered manually by an authorized person from a site, a region, an agency, or even the FRB. The transactional and blocked information is distributed to a POS based upon the site's position in the agency's hierarchy and upon an agency's policy. By default a location will receive all blocked records created at the location, all blocked records of the location's subordinate sites, all blocked records created at all direct ancestors above the location, and any blocked records from any location and their subordinates in the requesting location's location group.

In regards to transactional records, the location will only receive their own records and any transactional records originating at or below all locations, as well as any location and their subordinates included in the requesting location's Location Group. Upon processing a check, the POS application queries this information, known as the Local Verification Database or ("LVD"), for known negative payment history each time selected MICR information is read by the scanner.

What is Included in a Location's Policy?

A location's policy is based upon the agency overall program or policy to ensure a consistent application of an agency-wide check verification including returned reason codes, suspension periods, and the inclusion of expired items. As part of the agency's participation in the PCC program, the agency's central finance office provides the FRBC, via the Agency Site Profile (ASP), with a listing of return reason codes relevant to the agency, including:
- Number of returns permissible by the agency,
- Length of time for each suspension period.

This information is applied consistently across all locations for an agency's program.

The final piece of information required in a location's policy is what other locations are included in a location's LVD, known as the "location group". The location group typically includes locations from the hierarchy of respective location's agency, as well as, locations from another agency's hierarchy that may be in close proximity or service similar customers.

The location's policy is established during the set-up of a location in the MVD system. FRBC will administer the set-up of all locations based on the agency's and the location's Agency Site Profile (ASP). For the current version of the MVD, FRBC will administer all edits or modifications to a location, including the location's policy.

What Is CIRA

The CIRA contains an archive of all checks processed by participating agencies and locations of the PCC program. The archived batches originate from multiple POS applications deployed at various locations. During the Batch Close process, transactions are transmitted to the CIRA site and are available for viewing after twenty minutes. (Volume and system activity will affect the amount of time it will take to view your batch in the CIRA.) Authorized users can perform searches and view groups or specific checks that have been archived. Access to the CIRA is limited to authorized users due to the confidential nature of the items. For more information on CIRA, refer to *Using the CIRA* further in this section.

Accessing the MVD/CIRA

NOTE: The following procedures were written for Internet Explorer 6.0 (or higher), which is the recommended browser. If you are using Netscape 6.2 (or higher), the screens may look slightly different. Contact FRBC customer service with any questions at 216-579-2112 or 800-624-1373.

Login

Start your Internet browser (Netscape® 6.2 or Internet Explorer 6.0® or higher) and connect to the secure MVD/CIRA web address at https://www.mvd.gov *or* https://www.cira.gov . The following login appears when either URL is used:

® Netscape is a registered trademark of Netscape Communications Corporation.
® Internet Explorer is a registered trademark of Microsoft Corporation.

Enter your assigned Login Name and Password provided by FRBC in the boxes and then select OK to login. Only authorized users can gain access to the web application. Select reset to clear the login and password fields. You may also change your password on this screen by selecting the Change your Password link.
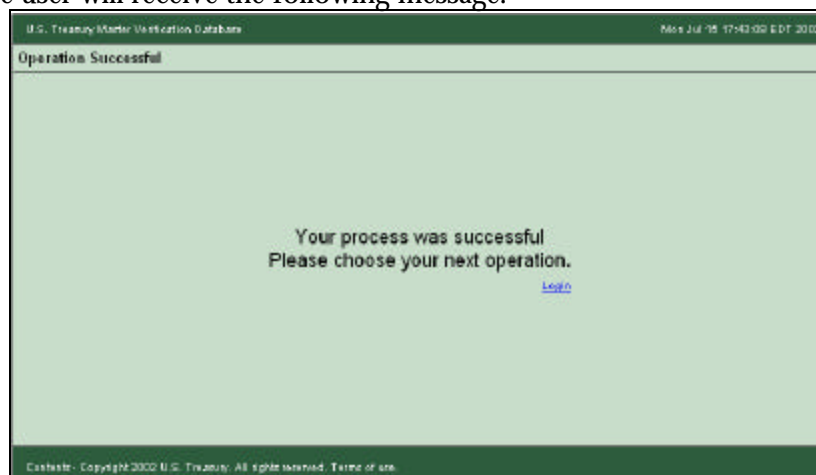
Password Administration

Upon initial login, the MVD/CIRA will require the user to change their password, as shown in the screen below:

The user must enter their User Name and old password, enter the new password twice for validation, then select OK. The password must be a minimum of eight characters, maximum of twenty-two characters, contain no spaces, and must include a combination of letters and numbers. No special characters should be used.

If the new password meets the criteria for passwords and has been entered successfully into the MVD/CIRA, the user will receive the following message:

Select Login to return to the Main screen, then enter your login and new password to access the MVD/CIRA.

The MVD/CIRA requires that user's password be changed every 30 days. Upon reaching the 30th day, the MVD/CIRA will prompt the user to change their password upon login. The new password must be different from the previous three passwords that have been used.

Password Reset/Account Lock

If a user account is locked and a password needs to be reset for the MVD/CIRA, call the FRBC Customer Service at 800-624-1373, 216-579-2112, or for military personnel, DSN 510-4-2-86824, option 6, option 4. Monday through Friday, from 8:00 a.m. to 8:00 p.m. ET. An FRBC Information Security staff member will call the user back, and provide the user with the new password. ***Note: This does not include the resetting of your PCC POS password. Only your on-site administrator can reset your PCC POS password by accessing the PCCSAT (System Administration Tool). Your on-site administrator can also assist you with your operating system password.***

CIRA/MVD Main Screen

Once you have successfully logged in, the MVD/CIRA main screen or "home page" displays. The screen may look different depending on your login access.

Note: The menu selections are determined by your access levels. Only the permissible menu options will appear for a user's logon ID. If there is a missing menu option for a user, that user does not have access to that option/function.
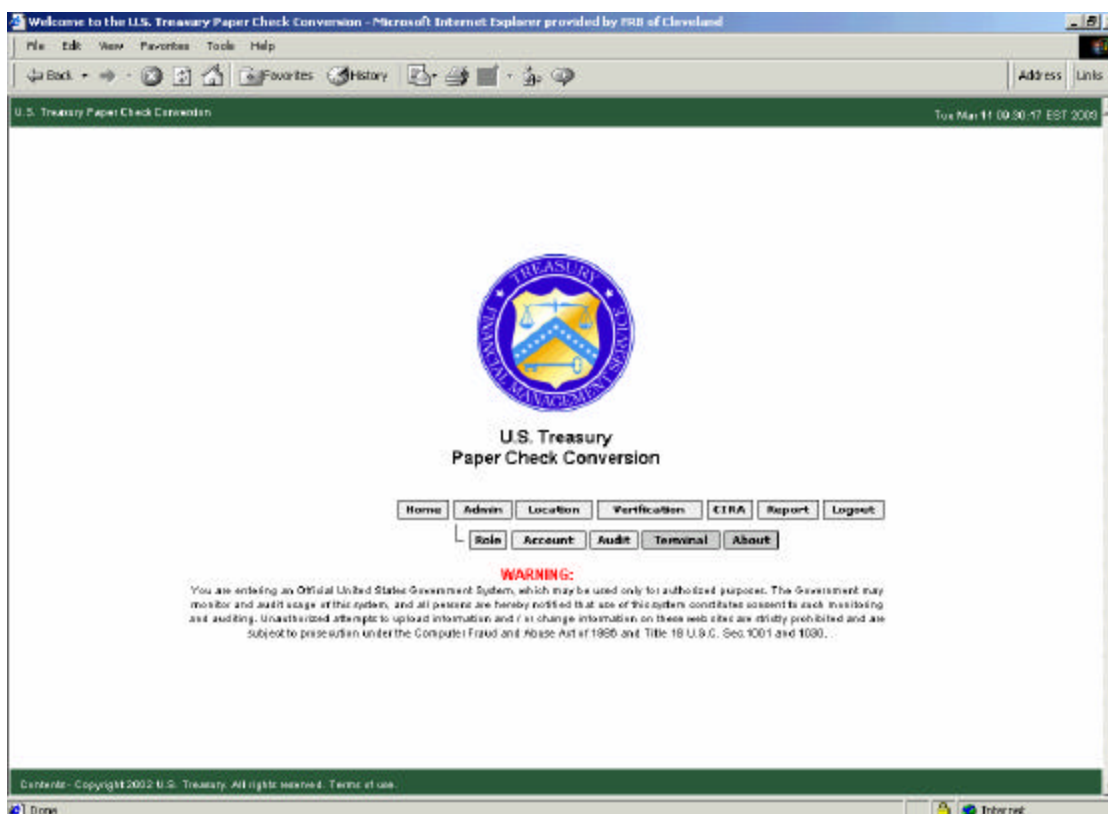
From this screen, the user can access the areas of the MVD/CIRA that are allowed based upon the permissions established in the role assigned to the user.

NOTE: In the current version of the MVD/CIRA the Terminal and About options are not functional.

Administration

Adding a User

To add a user to the MVD/CIRA, complete the Change Request Form in the *Appendix* and submit it to the Federal Reserve Bank of Cleveland as indicated on the form. Indicate on the form the level of access necessary for each user, i.e., if the user should have permission to request reports.

Deleting a User

To delete a user in the MVD/CIRA, send an email to PCC@clev.frb.org, including the user names that no longer need access for your location. You can also fax a CIRA/MVD change request form (See Appendix F) to 216-579-2003 or 216-579-2125.

Access Request

The administration of locations, users, and roles are performed by FRBC's staff. Please contact FRBC at 800-624-1373, 216-579-2112 or DSN 510-4-2-86824, option 6, option 4. Authorized users can view and monitor the information as described later in this section. Refer to *Viewing Information in the MVD.*

Location Management

Authorized users can select Location on the main menu to access the Location Management screen. Depending on your initial agency setup, the location view may not be available. An agency and location's policy is critical to understanding the verification process on checks presented at the POS terminal.

The agency's central financial management office, in coordination with a particular site, will establish the configurations for the following: relevant types of negative returns; the number of allowable returns; the length of the suspension period; and the other locations captured in a location's distributed verification database. This information will be entered into the MVD/CIRA by the FRBC operation staff in the location management section of the MVD/CIRA.

To view the location information, select Query from the Location Management screen, then select 'Detail' for the specific location. The following information displays:

| U.S. Treasury Paper Check Conversion | | | | Thu Mar 13 15:43:19 EST 2003 |

Location Management:

Home | Admin | Location | Verification | CIRA | Report | Logout
Role | Account | Audit | Terminal | About

Location Query
Please make your selection:
_____ Query | Reset

Location Results

Location	Parent Location	Detail	Description
0000789501	FederalReserve	Detail	Test Agency 4

Location Detail

Location Name:		Parent:
0000789501		FederalReserve

☑ includeExpiredCounts

Filter		Policy Holder:	0000789501
01			
02			
09			
11			

Description
Test Agency 4

Suspension		
1		0
2		3
3		1

Location Group	Group Holder:	0000789501
0000789502		
8300000101		
0000789501		

Return Reason Codes. See *Appendix* for descriptions

Suspension occurrence

Suspension period in number of days

Location Group
The locations included in a location's group represents a listing of any locations, outside the requesting location's hierarchy that is deemed relevant to include, verification records, and transactional and blocked records in the LVD for the requesting POS terminal.

Filter
The filter is how the agency specifies the return reason codes relevant to the agency's program. These codes represent the numeric codes used in the ACH return processing, which specify the reason for the return of the transaction. For example, code '01' means Non-Sufficient Funds, '02' means the account is closed, etc. Individual locations may apply additional filters (with FRBC assistance) outside the agency's required filter to suit the specific needs of the location.

See the *Appendix* section for a list of ACH return reason codes.

Suspension
A Suspension level specifies the number of calendar days that an individual will be unable to cash a check or pay by check and is calculated from the date the system is aware of the return file. The first suspension level is applied the first time a returned check with the defined return reason code is received into the MVD. The second suspension level will be applied to the second occurrence of a return when it is received on the respective account or other agency specified verification field, i.e. Social Security Number, Loan Account; and so on for the number of suspension levels that are defined for a particular location. After all the suspension levels have been exceeded, the individual will be denied from cashing a check.

Expired Accounts
The 'Include Expired Counts' flag indicates whether or not previous suspensions that have since expired (i.e., the individual is no longer suspended) are counted when assessing the suspension level to assign when the individual writes a check. .

Data Privacy

In addition to the filter, suspension, and location group setting, a location is able to establish their Data Privacy Policy, which defines the extent that users from other locations are able to view their verification records. This is accomplished the same way that role definitions are created to impose restrictions on what a user can view:

Attribute Descriptions:
    Note - Notes added to blocked or transactional records
    RT - Routing Number
    Loc Tag – (Location Tag) Site where record originated
    Account – Account number
    UserField1 – The first configurable field. While an agency may use more than one configurable field, only the first configurable field is included in the MVD.

Data Privacy allows the location the ability to control what fields of their verification records can be viewed by outside users. By default, all fields are set to "Block". For maximum data privacy, all fields would be marked as blocked, except Loc (Location) Tag. However, there may be situations where it is acceptable for outside users to view certain fields of verification records.

Any users at ancestor locations are not affected by this setting. Such users in general have complete control including edit capability (where applicable) over all fields of verification records originating at subordinate locations. Users from ancestor locations may be restricted based on their roles.

In establishing the Data Privacy Policy, it should be noted that in a situation where a user's role imposes different restrictions on accessing these fields from what is configured in the location detail, the more restrictive permissions shall apply.

To summarize, using the diagram below, if location F is in location D's location group then a user at location D will be able to view verification records originating at locations D, G, H, F, I and J as well as all Block records originating everywhere except at locations E and B. The data privacy settings established at location F will control what fields in the verification records the user at location D can see when viewing records originating at location F only. Separate settings at locations C, I, and J will control how location D sees records originating from those locations.
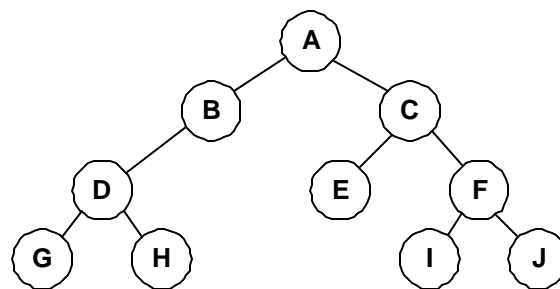
Dynamic Records

The status of a dynamic record reflects the policy of the location that processes the check; therefore, the status of a dynamic record changes according a specific location's policy. If the trading status of a dynamic record is changed manually (from D-Denied, D-Suspend to Denied, Suspend, or Clear), the record is no longer dynamic. The changed record will maintain the manually assigned status and will no longer reflect any other location's policy.

Verification

Verification management gives you access to the individual transaction records in the MVD. Depending on your permissions, you may be able to view and/or modify the trading status and other parameters of an existing transaction.

Verification records originate from returns on previous processed payments originated through the PCC system and manually entered records (i.e. block record). A subset of the MVD, based on requesting location and defined configurable filter parameters, is forwarded to the local field POS application. Blocked data is entered manually by an authorized person from a site, a region, an agency, or even the FRBC. The transactional and blocked information is distributed to a POS based upon the site's position in the agency's hierarchy and upon an agency's policy. By default a location will receive all blocked records created at the location, all of the location's subordinate sites, all blocked records created at all direct ancestors above the location, and any blocked records from any location in the requesting location's location group.

In regards to transactional records, the location will only receive their own records and any transactional records originating at or below all locations, as well as any location included in the requesting location's Location Group. Upon processing a check, the POS application queries this information, known as the Local Verification Database or ("LVD"), for known negative payment history each time selected MICR information is read by the scanner.

Status of Verification Record

An individual's ability to use PCC depends on the status in the system, which is a combination of the person's actual returned item history and the requesting site's policy. The status can be in one of five possible states:

- *Dynamic:* The status (D-Denied or D-Suspend) and deny date for each transactional record is based on the current policy of the requesting location. If the record status is edited, the record is no longer Dynamic. The changed record will maintain the manually assigned status and will no longer reflect any other location's policy.
- *Clear:* Prior restrictions on the individual's check payments have been removed. Select 'Clear' to reflect no status.
- *Suspend:* Suspend means an individual's record is set to a predetermined suspension period. During this time, the POS system will prevent an individual to cash a check through PCC. The individual's database record will have a Trading Status of Suspend and the expiration date will be set until a specific date.
- *Denied:* The expiration date defaults to a maximum date (9/9/2099). Currently upon receipt of a return, "Account Closed" return reason code (R02), the MVD automatically creates a record with a Denied status against the transactional record's account regardless of the location's policy or suspension and filters. The Deny status will be applied on any other transactions that can be linked to the closed account.
- *Blocked:* Indicates a manual entry by authorized persons into the MVD rather than the result of a failed transaction. If desired, an authorized user can edit the transactional record to a clear status.

Searching Verification Records

Since the MVD can potentially contain thousands of records, the ability to clearly define a search will result in better system results. Search results can be defined to limit the amount of data you will retrieve by entering criteria in the Search window.

- IRN - Unique 'item reference number'
- Userfield1 – Agency's specific first configurable field
- RT – Routing/transit number for the account associated with a transaction
- Account – Individual's account number
- Trade Status – Select a specific trade status from the drop down menu (Blocked, Suspend, Denied, Cleared, Dynamic, All). Refer to *Trading Status* for further explanation.
- Location – Location of requesting user
- Capture Date – Range for the capture date

Select [Query] to search based on any of these criteria. Alternatively you can click [Latest] to view the latest 100 records. When Latest is selected, no other search criteria apply. Select [Reset] to clear the search criteria.

Based on the type of query requested, the MVD provides the appropriate information matching your criteria. The following screen displays the results when an authorized user requested the verification records for a Blocked trade status and a specified capture date range.

The search results include transactions from the requesting location, subordinate location, and a location defined in a location group, i.e. site agreeing to share data.

NOTE: Currently the parent's transaction records are also included in the search results, yet the parent's transaction records are not included in the LVD download unless the parent is included in the location group.

The display is limited to twenty records per page. Use the scroll bar on the right of the Verification List window to view all 20 records. If there is a result of more than twenty records, select Next 20 to view the remaining records, then Previous 20 to view the previous records.

Print Records
To print all or part of this list, check the boxes to the left of the records you want to print or click Select All to print all records displayed on the current screen. Select Reset to deselect items. If there is more than twenty records, you must select and print the records displayed on each screen separately.

Click Print to display the selected items in a printer friendly format.

Select Print again to print the information. A print dialogue box displays. On the print dialogue box, select the desired printer and print criteria, then select Print.

Select BackList to return to the Verification List screen. If there is more than twenty records, the screen that you were printing records from displays.

Record Detail
To view the record detail for one or multiple records, check the boxes to the left of the records you want to view or click Select All to view detail of all the records displayed on the current screen. Select Reset to deselect items. Click Detail to view the selected record detail. If there is more than twenty records, you must select the records then select detail on each screen separately.

The following window appears, when detail is selected:

Only authorized users may edit the record. Refer to *Modifying Verification Records*.

If you selected more than one record, select Next at the bottom of the record detail window to view the detail for the additional record(s).

Select Previous to view the previous record(s).

Select Backlist to return to the Verification List screen. If there is more than twenty records, the screen that you were printing records from displays.

Modifying Verification Records

NOTE: The record no longer will be Dynamically marked if the trading status of a transaction is edited from D-Denied or D-Suspend to Suspend, Denied, or Cleared.

The ability to edit a verification record is based upon a user's role, as well as the location the user is assigned. That is, a user may be able to view another location's records, but any users below or outside a location's branch are not permitted to modify another location's verification records.

To modify transactional entries in the MVD, click Verification on the main menu, enter the search criteria, then select Query. Alternatively you can click Latest to view the latest 100 records. When Latest is selected, no other search criteria applies. The Verification List screen displays.

To view details on a particular record, check the box to the left of the record and then click Detail. The Verification Detail window for the selected record will be displayed. To modify the details of the selected transactional record, select the Edit button at the upper right hand corner of the Detail window to access the transactional record fields.

NOTE: An authorized user can only edit a record for their location or a subordinate location. Therefore, if the user is viewing other unauthorized location record detail, the Edit button will not display.

Once an authorized user selects Edit, the MVD will provide the following screen with a Verification Info window:

In the Verification Edit window you can change the following:
- Trade Status associated with this transaction. The trade status options available on the drop down will depend on the existing transaction record trade status.
- Deny Date, which is the date the current suspension will expire. Available only for non-dynamic records

- Override the setting that provides a field supervisor the ability to override an existing suspension. The edit availability depends on the existing transaction record trade status.
- Return Reason Code for this transaction
- Description for the Return Reason
- General comment to the transaction can be added or modified

Click Confirm to save your changes, Reset to return to the original settings, and Back to return to the record detail window.

NOTE: Currently if the 'Latest' button is used to display record results and you choose to edit a record from that listing, an error message appears once you confirm the edit. Even though an error message appeared, the change was applied. Select Latest from the Query window to verify the record changed.

Adding a Blocked Record

If an Agency needs to block a person, account or routing number from going through the verification database, a form needs to be completed and faxed to the Treasury (FMS) at 202-874-8644. This form is called the 'Add Blocked Record Request' and can be found in Appendix K.

Viewing Information in the MVD

Viewing Verification Records

In order to protect the privacy of a location's records included in the MVD, as part of a location's management configuration, locations can limit other locations ability to view all or certain data.

To view entries in the MVD, refer to *Searching Verification Records* as described earlier in this section.

Viewing Locations

Depending on your initial agency setup, the location view may not be available. To view a location, location hierarchy, or a location detail, the authorized user must query the MVD for their location or a subordinate location in their hierarchy. Select Location from the menu to access the query screen displayed below:

Enter the desired location's ALC + 2 (agency's location code predefined for the PCC program) on the location query screen, then select the Query to view the results or Reset to clear the information as presented in the illustration below:

The Location Result window displays:

The location named "Test Agency One" was located and the summary record for it appears to the right of the search box. If the desired location is a parent node in the hierarchy, the name will be a hypertext link to a listing of subordinate locations. If you leave the location name blank and just select Query, the system will return the record for the requesting user's location.

To view the location detail for the user's respective location, double click on the highlighted location name, actually the location's ALC+2, which is "8300000101": Selecting the location will generate a table showing all the direct child nodes of the location. In this case, the following screen appears:

U.S. Treasury Paper Check Conversion			Mon Mar 17 09:03:43 EST 2003
Location Management:		Home | Admin | Location | Verification | CIRA | Report | Logout	
		Role | Account | Audit | Terminal | About	
Location List			
Location	Parent Location	Detail	Description
8300000101	CIRA Query Test	Detail	Test Agency One
8300000102	8300000101	Detail	Test Agency Two

This example shows that the "Test Agency One" location has one direct descendant, "Test Agency Two". If any descendants are themselves parents, their names will appear as hypertext links. The user can click this name to view the location's descendent(s), and so on, to view the entire location hierarchy. Locations that do not have descendents, children or leaf nodes, will appear in the list as a simple name, not a hypertext link, as illustrated for "Test Agency Two".

By selecting the Parent Location hyperlink from the Location Result window, a detail window displays all the descendents of that parent location and indicates the Parent of that location, which in the example below is "Federal Reserve".

U.S. Treasury Paper Check Conversion			Mon Mar 17 09:04:59 EST 2003
Location Management:		Home | Admin | Location | Verification | CIRA | Report | Logout	
		Role | Account | Audit | Terminal | About	
Location List			
Location	Parent Location	Detail	Description
CIRA Query Test	FederalReserve	Detail	CIRA Query Regression Test Locations
8300000101	CIRA Query Test	Detail	Test Agency One
0000646901	CIRA Query Test	Detail	Test Agency Three
8300000113	CIRA Query Test	Detail	Test Agency 13
8300000115	CIRA Query Test	Detail	Test Agency 15
1304000101	CIRA Query Test	Detail	Census Test

To view the detail information of the location's set-up policy within a location's hierarchy, select the 'detail' for the location. In this case we are selecting a location named "Test Agency One", enter "8300000101". If the location entered is included in the user's location hierarchy, a screen similar to the following appears:

U.S. Treasury Paper Check Conversion				Mon Mar 17 09:46:11 EST 2003
Location Management:			Home | Admin | Location | Verification | CIRA | Report | Logout	
			Role | Account | Audit | Terminal | About	
Location Query		**Location Results**		
Please make your selection:	Query | Reset	Location	Parent Location	Detail	Description
		8300000101	CIRA Query Test	Detail	Test Agency One
		Location Detail		
Location Name:	Parent:			☐ IncludeExpiredCounts
8300000101	CIRA Query Test			
		Filter	Policy Holder:	8300000101
Description		01		
Test Agency One		02		
		03		
Location Group	Group Holder:	8300000101	Suspension	
8300000101		1	30	

The detail screen provides a summary of the requested location/verification policy. Refer to *Location Management* in this section for more detailed screen information.

View User Roles

All users are assigned a role that provides a set of predefined permissions. Role definition makes it easy to create and apply roles for several users, all of who are to have the same permissions and access rights.

In the MVD, user role definitions are established and edited by the Federal Reserve Bank based upon an agency's requirements. FRBC will maintain the set of agency's roles, and will designate which roles are available to a location in the creation of user accounts. A user at a location will only be able to view roles assigned to their respective location or to roles assigned to locations subordinate to the requesting locations. Select Role from the menu to view existing role definitions. The following screen appears:

To view the permissions and access rights for an existing role, click the arrow in the drop-down list box and select the role name (CIRAOnly, Edit, or View) in which you are interested. Then click Role Search. The following screen appears when searching on the Edit role:

The Role Permissions table shows check marks for the functions that this particular role has permission to perform. The Blocked Fields table shows permissions on individual attributes of a particular function.

Select Cancel to return to the Role Search screen.

To view roles assigned to a particular location, enter the location's ALC+2 or the location name into the role query on the Role Management main screen, and select ViewRole. The following screen displays:

View Users Accounts

Authorized users will be able to either search on a specific user's name or by all the users for a specified location. Similar to viewing roles, an authorized user will only receive user accounts matching query criteria that are associated with locations at or below the requesting user's location. To obtain a list of users per location, select Account from the menu. The following screen displays:

Enter the location's ALC+2 into the query box, and select OK. The MVD will provide a listing of users for the selected location, as displayed below:

To view the permissions for a particular user, select the user name on the Display Users window, or enter the user's login ID in the User Name box then select OK. If the user name that you entered is found, the user's name, location and role displays. When the user name is selected a screen appears displaying the detailed user profile:

Display Users		
User Name	Location	User Role
Testview3	0000646901	View

Search For Users

By user name:

[   ] [OK]

[Reset]

By location:

[   ] [OK]

[Reset]

User Detail Screen

User Profile

UserName:	Testview3
Description:	Regression Test
Role:	View
Location:	0000646901

Role Permissions:

Object Name:	Create:	Read:	Update:	Delete:
User Account	☐	☑	☐	☐
Verification	☐	☑	☐	☐
Location	☐	☑	☐	☐
UserLog	☐	☑	☐	☐
Role Account	☐	☑	☐	☐
Cira	☐	☑	☐	☐
Report	☐	☑	☐	☐
SystemConfig	☐	☐	☐	☐

Blocked Fields

Object Name:	Attribute:	Capability:

Using the Central Image Research Archive (CIRA)

Once the user selects the CIRA button form the Main screen, the user is presented with the site's custom main search screen:

NOTE: Your agency's logo will appear on the top of this screen.

Searching for Items

The CIRA search screen is designed so users may search by Agency Location Code (ALC+2) or by other criteria pertaining to desired results.

Accessing an agency query page is based on the location in the location hierarchy associated with the user. However, a user at a location higher in the location hierarchy is able to open a custom agency query page for any of the subordinate locations.

The **Location Name** is the ALC +2 (specific to a location), but it may also be the name of an Agency. The CIRA search screen will be customized with your location name and logo.   If your logon ID allows you to see many sites for your particular organization, you may need to specify a location for specific querries. . The search results will also include the ALC's subordinate locations if 'Include Subordinate Locations' is checked.

Search for checks by one search criteria, or by a combination of criteria. ***NOTE: At least 1 field needs to be entered in order to perform your search.*** The more search information input, the more refined your search results will be.

- **Configurable Fields** – The first four Agency specific configurable fields, which are specific to your agency, may be searched. The field labeling and search type will be aligned to the field definitions for location being searched. The fields may consist of text, date, number, and currency. A Number field provides a drop down with query options of Inclusive, Exclusive, Great Than, Less Than, and Equal To. A Date field provides a drop down with query options of Inclusive and Equal To. In the example above there are generic field representations.
- **Bank Account Number** – Bank account number on check. A search on an account may draw more than one account.
- **Bank Routing Number** – Bank routing number on a check. A search on Bank routing number may result in a large number of items as numerous checking accounts may be drawn on a single routing number.
- **Unique Transaction ID** – Also known as the Item Reference Number (IRN) which is tied to a specific transaction. Currently the width of this field does not allow the user to view the entire input value, but the input is not affected.
- **Cashier ID** – Cashier ID from POS terminal
- **Amount of Check** – Check Amount. Check Amount. A search on dollar amount could result in a large quantity of item results. It is encouraged that you use another search criteria along with amount of check.
- **Batch ID** – The batch ID assigned by the POS. Currently the width of this field does not allow the user to view the entire input value, but the input is not affected.
- **Received Date** – The date the check was received into the CIRA. Select 'Equal To' from the drop down menu to select a specific date and time (if desired), or select 'Inclusive' to enter a date range. Currently, to return the most recent records starting with a specific date, select 'Inclusive', then in the date range enter the earliest time possible and leave the second parameter clear.
- **Check Capture Date** – The date the check was processed by the POS terminal. Select 'Equal To' from the drop down menu to select a specific date and time, or select 'Inclusive' to enter a date range. Currently, to return the most recent records starting with a specific date, select 'Inclusive', then in the date range enter the earliest time possible and leave the second parameter clear.

NOTE: To search for a specific item, the IRN field can be used. This is a unique identifier for an individual check transaction..

After the user has entered the criteria, the following options are available:

- **View Items** - Select $\boxed{\text{View Items}}$ to view the results listing page and the image of the check. Refer to the *CIRA Search Results* for a screen example.
- **Count –** Select $\boxed{\text{Count}}$ to view the number of items in the database that matched the search criteria without displaying them. The following screen displays the item count and the total dollar amount:

- **Report** – This is button allows for a report request. For specific details pertaining to 'Reports' see
- **Reset –** Select $\boxed{\text{Reset}}$ to clear the search criteria to conduct a different search.

CIRA Search Results

When viewing the item search results, users will be able to view the image and all details pertaining to each individual check item. The following screen shows a typical search results screen. Note that if the search criteria match more than 1000 items in the archive only the first 1000 items will be returned. In this case you may wish to refine your search criteria through the use of different time periods in order to reduce the number of matches and allow the user to view the detail items. Select $\boxed{\text{View Items}}$ to display the following screen:

Listing section

Check Image section

Item Detail section

Results Screen Overview

Select 'File' then 'Print' to print the entire screen, including all sections. At this time, if no search results are available, a screen displays without any detail transactions.

Listing section:
- Only the first configurable field displays.
- Each column heading can be clicked to sort the list using that column as the sort key.
- Each Unique Transaction ID can be selected to view each item image and all associated item details.
- Each results listing page contains a maximum of 15 records. To view the next 15 records (if applicable) the user must scroll to the bottom of the listing section and select Next. Select Previous to view the previous 15 records.
- Select Back to return to the Search Criteria screen.

Check Image section:
- Displays image of the Unique Transaction ID selected in the Listing section.
- Each item image can be saved or printed by selecting the appropriate icon in the image window.
- Refer to the TIFF Image information for more details on viewing the check image.

Item Detail section:
- Displays item detail of the Unique Transaction ID selected in the Listing section, including all configurable field information. Use the scroll bar to view all the information.
- If the check was a business check or processed in Lockbox mode, select Next to view the back of the check then Previous to return to the front of the check view. If viewing a check processed in POS mode, these buttons do not display.

Can your Browser Display TIFF Images?

A user can select the link 'Can your Browser Display TIFF Images?' link, from the CIRA screen, to determine if the local PC has been set up to view TIFF images. The link is found at the lower left of the CIRA screen.

NOTE: When using Netscape, an error appears when this link is selected; therefore it cannot be used.

When the user selects this link they will be directed to a view check screen if successful. The page will be presented with following page containing a sample check. If the user can view the check, then the test has been successful.
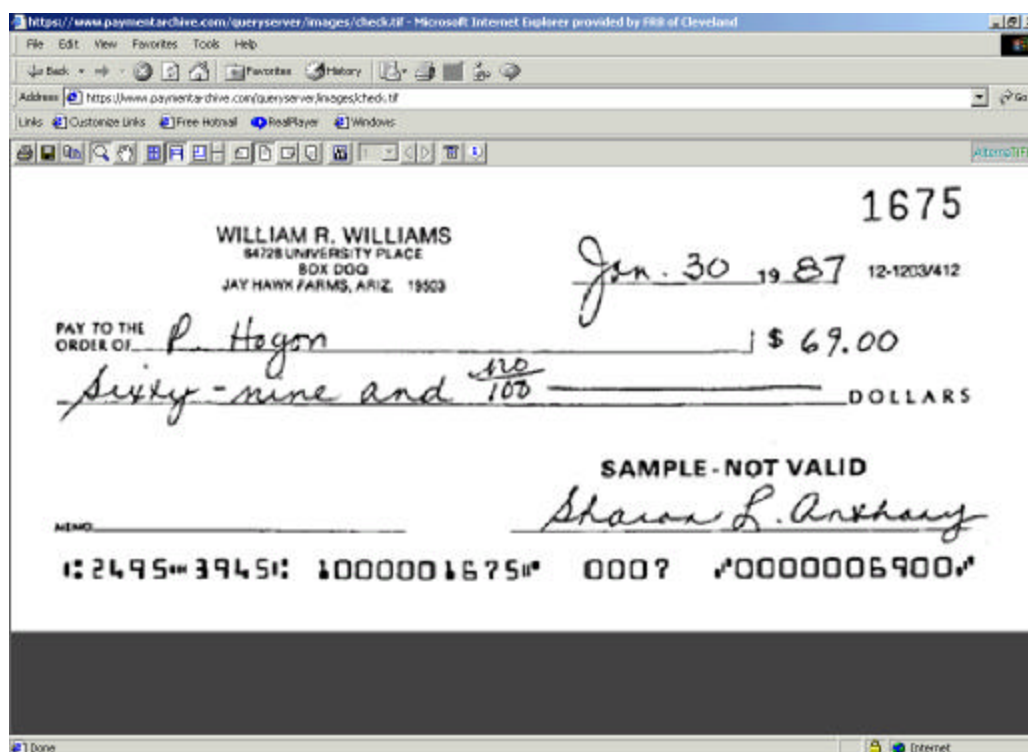
The user can select the 'Back' button on the browser to return to the main CIRA search screen.

If the user does not have the proper TIFF viewer installed on the local PC, the user will be presented with a blank screen.

To install the correct TIFF viewer, refer to *Setting up the TIFF Viewer.*

Setting up the TIFF Viewer

To install the TIFF viewer, an authorized user must select the 'AlternaTiFF' link at the bottom of the main CIRA search screen. The user will be presented with the following screen:
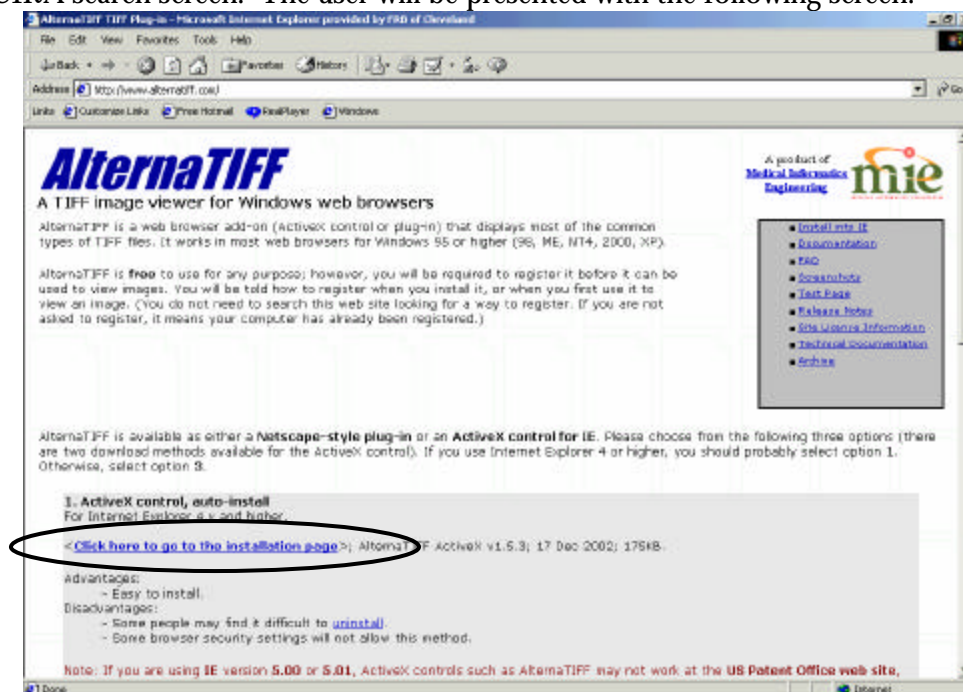
Users that do not have AlternaTiff already installed on their clients should download the appropriate Internet viewer from the AlternaTiff web site. For Netscape users, directly access the www.alternatiff.com web site.

The user must select the 'Click here to go to the installation page' link. Once the link has been selected, the user will be presented with the following page. Select the 'Auto-install AlternaTIFF ActiveX control' link to proceed. If your Agency allows Active X on your workstation, you may need to work with your system administrator to load the Tiff viewer on your workstation.
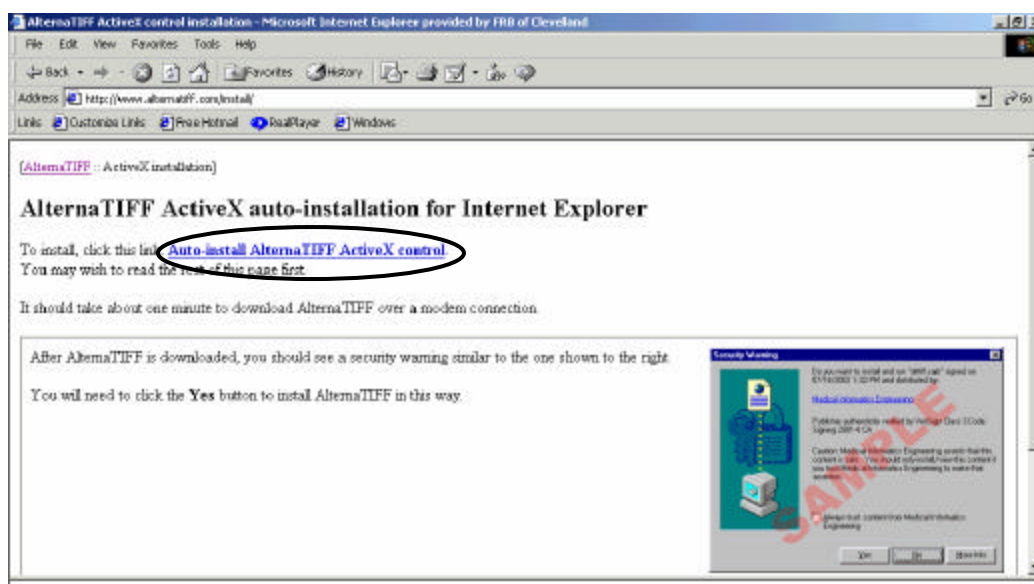
When the download is complete, the bottom section of the web screen will be updated and will state 'AlternaTIFF viewer ActiveX control is installed in your browser'. Click in the bottom section to return to the AlternaTIFF main page.

The TIFF viewer has now been successfully installed on the PC. To test this, the user can select the 'Can your browser display TIFF image files?' link on the main CIRA search page. The sample check image should now appear.

CIRA Report

The CIRA report is available in comma-separated value (CSV) format. It can be viewed using Wordpad, which is standard application on all PCC terminals, or another preferred application. Yet, if available, a spreadsheet application provides the most flexibility in viewing and manipulating the report data.

In order to view the CIRA results in a report format, enter the search criteria on the CIRA Query screen, then select Report. The CIRA report is available to anyone with access privileges to the CIRA.

NOTE: The following procedures are recommendations for viewing the CIRA report CSV file using the Excel® spreadsheet application, yet the data can be viewed according to your preference by selecting other options on following screens.

On the File Download screen, select 'Save…' then select OK.

® Excel is a registered trademark of Microsoft Corporation.
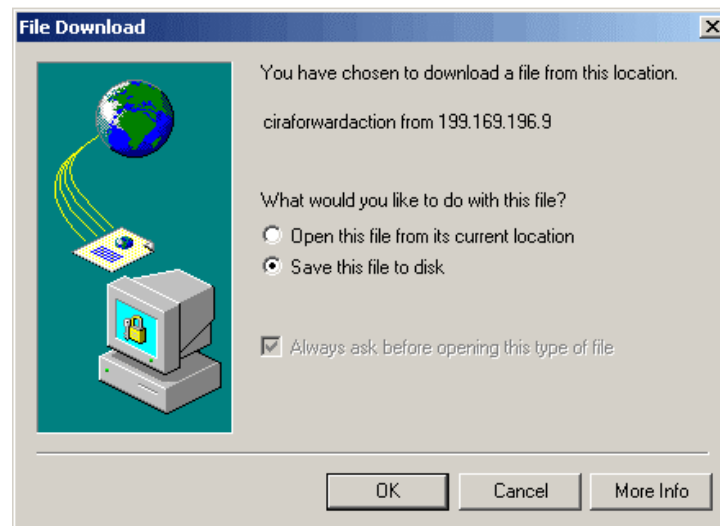
On the Save As dialogue box indicate where you want the file to be saved, verify if the file name and rename it if needed, then select ⬚Save⬚.

Note: Depending on the application you are using to view this report, the .csv extension may need to be added to the end of the file name. This is not needed when using the Excel application.
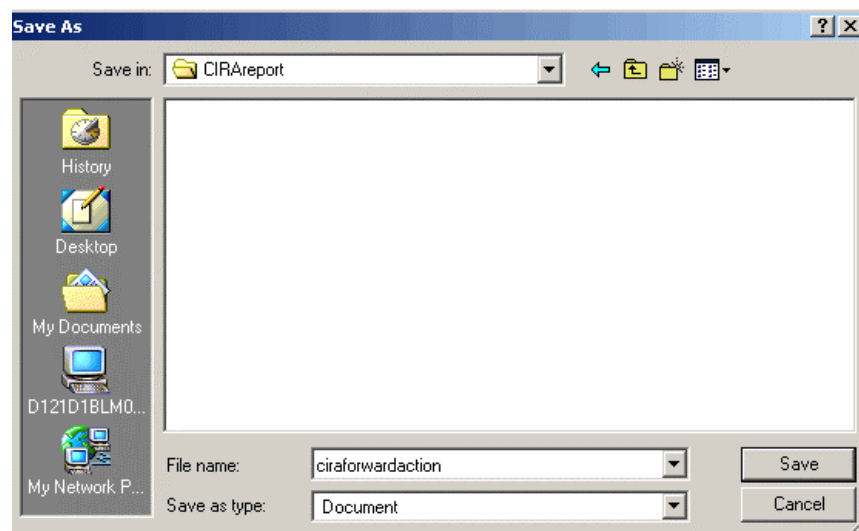
Select ⬚Close⬚ on the Download Complete screen.
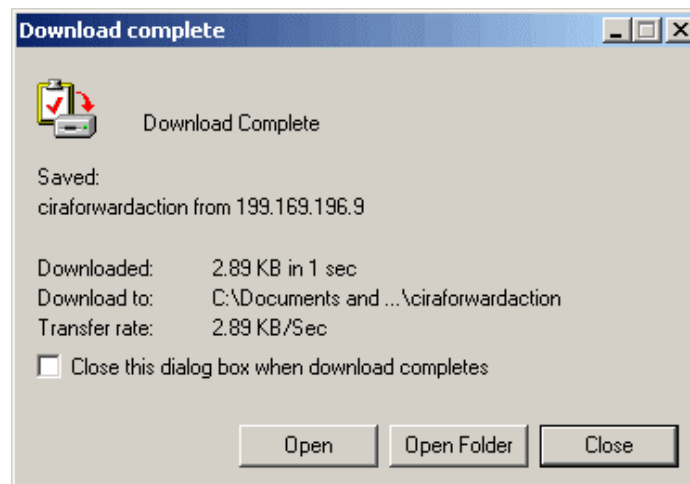
Launch the spreadsheet application, then select 'File', then 'Open' within the spreadsheet application.

On the Open dialogue box, locate the CIRA report that you just saved, the select $\boxed{\text{Open}}$. The File Type may need to be changed to "All Files" so the .csv file displays.
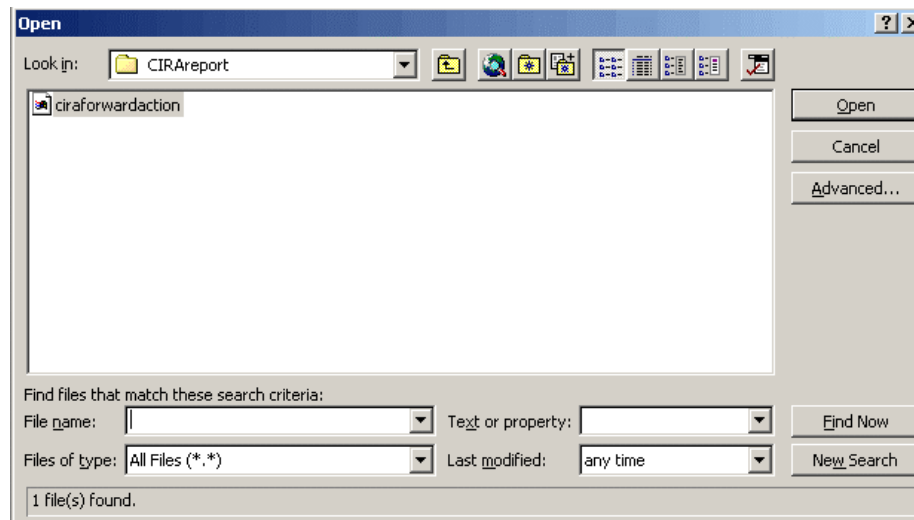
On the Text Import Wizard screen, select 'Delimited', then select $\boxed{\text{Next}}$.
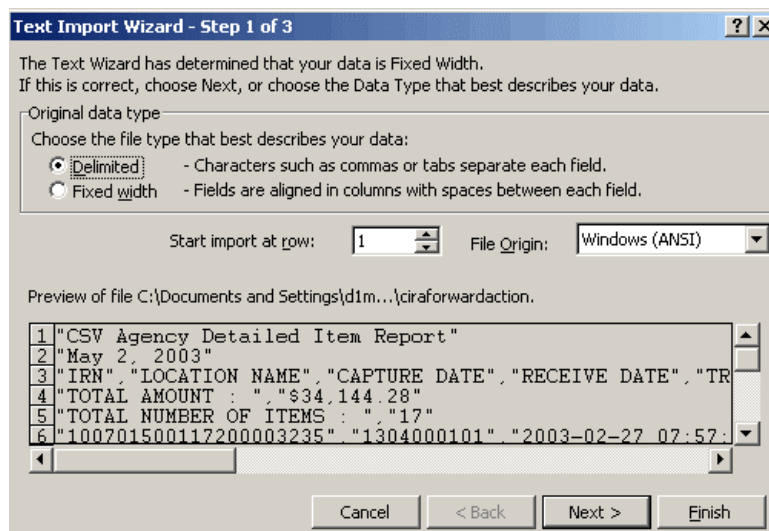
On the Text Import Wizard – Step 2 screen, select 'Comma' in the Delimited section so the data will be separated into columns on the spreadsheet wherever there is a comma in the report text. The text Qualifier should be (") which is the default. Select Next .

On the Text Import Wizard – Step 3 screen, select each column so that it is highlighted (use the scroll bar to view all the columns), then select "Text". Select Finish.

Note: The IRN column must be in Text format so that the entire IRN number displays. The other columns can be formatted according to your preference.

Below is an example of the spreadsheet. The column widths need to be adjusted to view all the information. Use the scroll bars to view all the data. The data can also be formatted and sorted just like any other spreadsheet and can be saved for your records.

	A	B	C	D	E	F	G	H	I	
1	CSV Agency Detailed Item Report									
2	May 8, 2003									
3	IRN	LOCATION NAME	CAPTURE DATE	RECEIVE DATE	TRANSIT NUMBER	ACCOUNT	AMOUNT	CASHIER ID	CHECK TY	PROCE
4	TOTAL AMOUNT :	$34,144.28								
5	TOTAL NUMBER OF ITEMS :	17								
6	100701500117200003235	1304000101	2/27/2003 7:57	2/27/2003 8:09	41212433	98409	$2,009.09	TestUser1	5	LOCKB
7	100701500117200003237	1304000101	2/27/2003 7:58	2/27/2003 8:09	41212433	98411	$2,011.11	TestUser1	5	LOCKB
8	100701500117200003239	1304000101	2/27/2003 7:58	2/27/2003 8:09	41212433	98412	$2,012.12	TestUser1	5	LOCKB
9	100701500117200003241	1304000101	2/27/2003 7:59	2/27/2003 8:09	41212433	98413	$2,013.13	TestUser1	5	LOCKB
10	100701500117200003243	1304000101	2/27/2003 7:59	2/27/2003 8:09	41212433	98414	$2,014.14	TestUser1	5	LOCKB
11	100701500117200003247	1304000101	2/27/2003 8:01	2/27/2003 8:09	41212433	98415	$2,015.00	TestUser1	1	LOCKB
12	100701500117200003249	1304000101	2/27/2003 8:01	2/27/2003 8:09	41212433	98416	$2,016.16	TestUser1	1	LOCKB
13	100701500117200003251	1304000101	2/27/2003 8:01	2/27/2003 8:09	41212433	98417	$2,017.17	TestUser1	1	LOCKB
14	100701500117200003253	1304000101	2/27/2003 8:04	2/27/2003 8:09	41212433	98400	$2,000.00	TestUser1	3	POS
15	100701500117200003254	1304000101	2/27/2003 8:04	2/27/2003 8:09	41212433	98401	$2,001.01	Test Supervisor	3	POS
16	100701500117200003255	1304000101	2/27/2003 8:04	2/27/2003 8:09	41212433	98402	$2,002.02	Test Supervisor	3	POS
17	100701500117200003256	1304000101	2/27/2003 8:05	2/27/2003 8:09	41212433	98403	$2,003.03	Test Supervisor	3	POS
18	100701500117200003257	1304000101	2/27/2003 8:05	2/27/2003 8:09	41212433	98404	$2,004.04	Test Supervisor	3	POS
19	100701500117200003258	1304000101	2/27/2003 8:05	2/27/2003 8:09	41212433	98405	$2,005.05	Test Supervisor	3	POS
20	100701500117200003259	1304000101	2/27/2003 8:06	2/27/2003 8:09	41212433	98406	$2,006.06	Test Supervisor	1	POS
21	100701500117200003261	1304000101	2/27/2003 8:06	2/27/2003 8:09	41212433	98407	$2,007.07	Test Supervisor	1	POS
22	100701500117200003263	1304000101	2/27/2003 8:07	2/27/2003 8:09	41212433	98408	$2,008.08	Test Supervisor	1	POS
23										

When viewing the data, note that the Check Type column displays the numbers 1, 3, and 5. These numbers represent the following:
- 1 - business check processed in Lockbox or POS mode.
- 5 - personal check processed in Lockbox mode.
- 3 - personal check processed in POS mode.

Select 'File', then 'Save' from the spreadsheet menu to save any changes as a spreadsheet file.

Report

The reports available are based on the user's role and location. Select Reports from the menu to access various MVD/CIRA reports. The following screen displays:

Note: In order for a user to request reports, prior authorization must be requested using the CIRA/MVD request form (Appendix G).

<table>
<tr><td colspan="2">**MVD Reporting Tools**</td></tr>
<tr><td colspan="2">**Select Report:**</td></tr>
<tr><td>Agency CIRA Report</td><td>○</td></tr>
<tr><td>LVD Contents</td><td>○</td></tr>
<tr><td>Location Hierarchy</td><td>○</td></tr>
<tr><td>Location Policy</td><td>○</td></tr>
<tr><td>Location Groups</td><td>○</td></tr>
<tr><td></td><td>**Submit Request**</td></tr>
</table>

To view a report, select the radio button next to the report, then select Submit Request.

Each report can be displayed in 3 output styles:
- HTML – Hypertext Markup Language is a "browser view" or "online view". An HTML file is intended for display on a browser page.
- CSV – Comma-Separated Values is a format that can be "machine downloaded" style. A CSV file is a way to collect the data from any table to be conveyed as input to another table-oriented application, including spreadsheet or relational database applications.
- PDF – Portable Document Format is a "printable download" style. A PDF file is a universal file format that can be shared, viewed, or printed exactly as intended by using Adobe Acrobat Reader® software. Read-only software is free and can be downloaded from the Adobe web site, www.adobe.com.

For the best print format, users should select the .pdf format. Printer setting vary; therefore, the preferences on the printer dialogue box may need to be adjusted (i.e. landscape vs. portrait).

The following information provides details about each report.

® Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Agency CIRA Report

This report provides a summary of PCC processed items for a requested location. Since the CIRA can potentially contain millions of records, a user should limit the amount of data retrieved by entering search criteria in the **Search Criteria** window.

An authorized user can search using the following:

- Location name – Enter location name, and check the box if any subordinate location's data should be included in the report.
- Date – Select the radio button for Capture Date (date check processed at site) or Received Date (date batch transmitted to CIRA) then enter the Date From and Date To.
- Batch ID – All is the default. Enter a specific batch ID if desired.
- Cashier ID - All is the default. Enter a specific cashier ID if desired.

Select the appropriate radio button in the **Specify Output Style** window to indicate the format to view, print or save the report.

NOTE: An authorized user will only receive information matching query criteria associated with locations at or below the requesting user's location.

Select Submit Request to view the report.

Agency CIRA Report
This report displays the transaction activity for specified location.
Search Criteria:
Location Name: `CIRA Query Test`
Include Subordinate Locations: ☑
Date From: `2003` `March` `17`
Date To: `2003` `March` `17`
Received Date: ⦿
Captured Date: ○
Batch ID: `ALL`
Cashier ID: `ALL`
Specify Output Style:
HTML: ⦿
CSV: ○
PDF: ○
Submit Request

Note: The CIRA report should be printed in a .pdf format.

Below is an Agency CIRA Report example in .pdf format:

```
                           Agency CIRA Report

 Location : CIRA Query Test                        Mar 17, 2003


 Daily Summary for all Locations :     Received Date  Item Count  Dollar Amount

                                         2003-03-17      50           ?82,666.0

    Grand Total :                                        50           ?82,666.0


   Received Date            2003-03-17

                          Location      # of    Received
 Location Name           Description   Direct   Date      Item Count  Dollar Amount
                                       Child

 CIRA Query Test  CIRA Query Regression Test Lc  5   2003-03-17   0        ?0.0C

 0000646901       Test Agency Three         1   2003-03-17   10       ?20,267.0

 1304000101       Census Test               0   2003-03-17   0        ?0.0C

 8300000101       Test Agency One           1   2003-03-17   40       ?62,399.0

 8300000113       Test Agency 13            1   2003-03-17   0        ?0.0C

 8300000115       Test Agency 15            1   2003-03-17   0        ?0.0C

    Total per Date :                                       50        ?82,666.0
```

LVD Contents

This report allows authorized users to produce a report that represents negative check data downloaded to the POS. The data provided in this report reflect the transaction status, as of the current date. Users of this report should be aware of the time sensitivity of the data.

An authorized user can request information using the following **Search Criteria**:
- Location – Location name, i.e. ALC+2
- Transaction Type – Use the drop down arrow to select transaction, block, or all.
- Trade Status – Use the drop down arrow to select all, suspend, blocked, denied.
- Account - User account
- Config Field 1 – The agency's specific first configurable field information.
- Bank RT number – Bank's routing/transit number

In the **Sort Order** window select a category using the drop down arrows to indicate the sort order for the report to be presented. The categories are Location, Trade Status, Account, and the specific Agency's first Configurable Field. Use the drop down arrows to sort these categories by either ascending (asc) or descending (desc) order. By using the sort order in the screen displayed below, the report will be produced by Location, then by Status of the item, then by Account, then by Agency Configuration 1 with all data sorted in ascending order.

Select the appropriate radio button in the **Specify Output Style** window to indicate the format to view, print, or save the report. Select Submit Request to view the report.

NOTE: An authorized user will only receive information matching query criteria that are associated with locations at or below the requesting user's location

LVD Contents

This report displays the contents of a Local Verification Database (LVD) for a given ALC+2.

Search Criteria:

Location Name:	CIRA Query Test
Transaction Type:	ALL
Trade Status:	ALL
Account:	ALL
Config Field 1:	ALL
Bank RT Number:	ALL

Sort Criteria:

Sort Criteria 1:	LOCATION	ASC
Sort Criteria 2:	TRADE STATUS	ASC
Sort Criteria 3:	ACCOUNT	ASC
Sort Criteria 4:	CONFIG FIELD 1	ASC

Specify Output Style:

HTML:	⦿
CSV:	○
PDF:	○
	Submit Request

Below is an LVD Contents Report example in .pdf format:

```
                                 LVD Contents

  Requsted by :     MarcieTestEdit@CIRA Query Test                    Mar 17, 2003
  Target Location   CIRA Query Test
  Date :            2003-03-17
  Num of records : 37


  Configurable    Routing   Account       Closed Denied     Trade    Override Capture Date       Location Description
      Field 1     Number    Number        Acount Until      Statue


  842**4786                                      2099-09-09  BLOCKED    Y     2002-09-25 00:53:11  Test Agency Three


  509**4321                                      2099-09-09  BLOCKED    Y     2002-09-25 00:53:40  Test Agency Three


  286**6519                                      2099-09-09  BLOCKED    Y     2002-09-25 00:58:39  Census Test


               ****12433  98400        Yes  2099-09-09  DENIED     Y     2003-02-27 08:04:23  Census Test


               ****12433  98401        Yes  2099-09-09  DENIED     Y     2003-02-26 12:37:01  Census Test


               ****12433  98406        Yes  2099-09-09  DENIED     Y     2003-02-27 08:06:05  Census Test


               ****12433  98406        Yes  2099-09-09  DENIED     Y     2003-02-26 12:38:45  Census Test


                                 For Official Use Only
```

This report includes sensitive and private information, and should be handled and discarded appropriately. Also the data on this report is time sensitive; therefore, aged reports should not be relied upon and discarded appropriately.

NOTE: Certain fields have been partially masked (****) to limit the viewing of sensitive information.

Location Hierarchy

The report provides an authorized user the ability to obtain and understand their location's hierarchy.

Enter the location and select the appropriate radio button in the **Specify Output Style** window to indicate the format to view, save, or print the report.

NOTE: An authorized user will only receive information matching query criteria that are associated with locations at or below the requesting user's location.

Select Submit Request to view the report.

Location Hierarchy

This report displays the target location within the context of the current location.

Specify Output Style:

Location Name:	CIRA Query Test
HTML:	◉
CSV:	○
PDF:	○
	Submit Request

Below is a Location Hierarchy report example in .pdf format:

Location Hierarchy

Home Location :   CIRA Query Test   Mar 17, 2003

Target Location : CIRA Query Test

___

Requested location hierarchy →

Ancestors of Location   CIRA Query Test   LEVEL

_____CIRA Query Test   1
CIRA Query Regression Test Locations

_____FederalReserve   2

Parent → *The Federal Reserve, root of the location hierarchy.*

Descendents of Location   CIRA Query Test

_____CIRA Query Test   1
CIRA Query Regression Test Locations

Subordinate locations →

_____8300000101   2
Test Agency One

_____8300000102   3
Test Agency Two

_____0000646901   2

Subordinate of one of CIRA Query Test's subordinate

NOTE: Subordinate locations are presented on the report in ascending order under the parent and have a higher level number, which indicates the level of the hierarchy.

Location Policy

This report lists a location's policy, including relevant returned check criteria, location group, definition of suspension periods, etc.

In the **Search Criteria** window enter the location and indicate if subordinate locations should be included.

Select the appropriate radio button in the **Specify Output Style** window to indicate how you want to view, save, or print the report.

NOTE: An authorized user will only receive information matching query criteria that are associated with locations at or below the requesting user's location.

Select Submit Request to view the report.

Location Policy
This report displays the location policies used in the feed processing and delivery processes.

Search Criteria:	
Location Name:	CIRA Query Test
Include Subordinate Locations:	☑
Specify Output Style:	
HTML:	⦿
CSV:	○
PDF:	○
	Submit Request

Below is a Location Policy report example in .pdf format:

```
                          Location Policy

                Target Location  CIRA Query Test

                Home Location    CIRA Query Test
                                                                  Level


     ┌─────────────────────────────────────┐                    ┌─────┐
     │ Location        CIRA Query Test      │                    │  1  │
     └─────────────────────────────────────┘                    └─────┘


            Policy Holde: FederalReserve

                      Include Expired Counts : False

                      Suspension Periods

                      Occurence :         Days :

                      1                   30


                      Suspension Periods

                      Occurence :         Days :

                      2                   60


                      Suspension Periods

                      Occurence :         Days :

                      3                   90


                      Acceptable Return Reason Code.

                      Filter :            RRC :

                      01                  Insufficient Funds

                      02                  Account Closed

                      09                  Uncollected Funds
```

Location Groups

This report provides a listing of all locations that the requesting location can view in the MVD, and is included in their LVD downloads that are outside of their location hierarchy.

Enter the location and select the appropriate radio button in the **Specify Output Style** window to indicate how you want to view, print, or save the report.

NOTE: An authorized user will only receive information matching query criteria that are associated with locations at or below the requesting user's location.

Select Submit Request to view the report.

Below is a Location Group report example in .pdf format:

Terminating Your Session

To terminate your connection to the MVD/CIRA system click Logout on the main menu, then close the application browser. If a user does not logout through the logout button, the secure SSL session will expire. In order to re-enter the application/system, the user will be locked out and must wait 15 minutes. Note also that your session will expire automatically after fifteen minutes of inactivity.

Future Enhancement - Terminal Management

Selecting Terminal will allow you to view information about individual POS terminals and to block terminals from receiving LVD updates.

United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Reporting and Balancing with CA$H-LINK

Revised October 8, 2003

Table of Contents

Reporting and Balancing with CA$H-LINK

Overview

The CIRA web site provides the ability to view transactions based on several criteria. On a daily basis items received by 9:30[1] EST will be forwarded on to FedACH[2] for payment collections. All transactions sent to the CIRA since the last business day will be forwarded to the Federal Reserve Bank of Cleveland for further processing. Transactions will be processed at the Federal Reserve's Automated Clearing House system, known as FedACH. FedACH will send a debit ACH transaction to the check writer's financial institution. The following business day, an SF215 deposit ticket will be credited to your agency's CA$HLINK account. The Federal Reserve System feeds into Riggs CA$HLINK at the end-of-day. You will see activity in Riggs on the third day with the effective entry date matching your SF215 that FRB Cleveland provided. All PCC activity will be reflected in CA$HLINK as activity from 0420 which is the Federal Reserve Bank of Cleveland's Cincinnati office.

NOTE: Federal Reserve Bank of Cleveland business days are Monday thru Friday, except holidays. To view holiday dates, please go to www.clevelandfed.org/about/Holidays.htm.

Daily Reports

Three reports will be delivered to the appropriate agency contact through email from FRBC each business day. These include:

- The SF215 Report for all items being deposited into CA$H-LINK on that day. The SF215 report will contain detailed information with the number of transactions, dollar amount, transaction date, cashier ID, and location that add up to a single deposit for an ALC/DSSN. The single deposit ticket per location will batch ACH and paper origination items.

- The SF5515 report will contain the debit voucher number for each item that is retired by the Federal Reserve Bank. The report provided includes detailed information on the Unique Transaction ID (or IRN number) for easy research on the CIRA site.

---

[1] These times are subject to change based on the volume of transactions being processed. If this time changes the appropriate agency contact will be notified 30 days prior to the change.

[2] FedACH or ACH (Automated Clearing House) is a computer-based clearing and settlement operation, often operated by a Federal Reserve Bank, established for the exchange of electronic transactions among participating depository institutions. Such electronic transactions can be substituted for paper checks used to make recurring payments such as payroll or preauthorized insurance premiums. The U.S. Treasury uses the ACH extensively to pay certain obligations of the government.

- The Daily Checks Pending Redeposit Report reflects the first time an item has been returned but will be based on the represent schedule selected by the agency during the pre-deployment process.

A sample of each of these reports is available in the *Appendix.*

Problems Balancing to CA$H-LINK

Each day, SF215 and SF5515 information will be emailed to the designated agency contact (i.e. Regional Accounting Manager or Disbursing Officer). If this information on the SF215 does not match what was transmitted to the CIRA:

- Determine the time that the information was sent to the CIRA. Currently, if this is prior to 9:30 p.m. EST, the batch of transactions will be contained on the SF215 form on the next day.

- Currently, if all transactions were sent prior to 9:30 p.m. EST but are not on the SF215 form, please contact the Federal Reserve Bank of Cleveland at 800-624-1373 or 216-579-2112 or at pcc@clev.frb.org.

NOTE: If unable to match to information provided on the SF215 or SF5515, please contact the Federal Reserve Bank of Cleveland with the dates and ALC numbers of the locations having problems balancing.

Also:

If your site has large dollar transactions, please ensure that you see the items in the CIRA on the same day that you transmit them. This ensures that the batch transmitted successfully and will provide you with a level of confidence that you will obtain your Ca$h-Link deposit the next business day.

United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Troubleshooting

Revised October 8, 2003

Table of Contents

Troubleshooting

NOTE: An email must be sent when reporting problems for items referred to the Federal Reserve Bank of Cleveland.

Hardware and SF Form 215/5515 Troubleshooting Process

```
                              ┌─────────────────────┐
                              │        FRB          │
                              │    CLEVELAND        │
                              │   216-579-2112      │
                              │   800-624-1373      │
                              │  DSN 510-4-2-86824  │
                              │   press 6, then 4   │
                              └─────────────────────┘

┌──────────────┐   ┌──────────────┐   ┌──────────────┐   ┌──────────────┐
│Agency Central│   │              │   │     SOP      │   │   Regional   │
│  Accounting  │ ← │   System     │ ← │Troubleshooting│ ← │Accounting or │
│  Group or    │   │Administrator │   │   Section    │   │  Finance     │
│Agency Liaison│   │              │   │              │   │  Manager     │
└──────────────┘   └──────────────┘   └──────────────┘   └──────────────┘
```
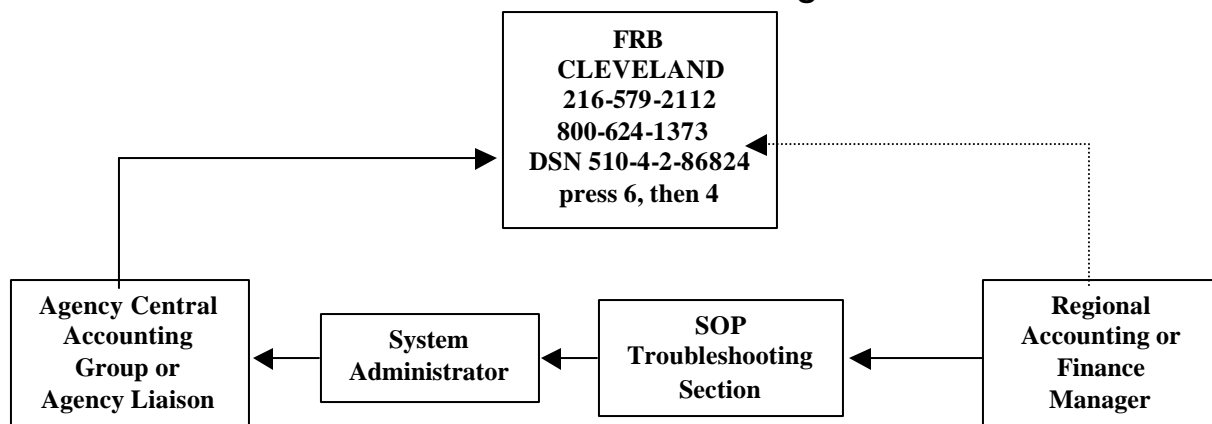
Contingency

A contingency plan is a must. Stateside agencies can contact FRB to have a scanner sent to them overnight to your disaster relocation site in the event it is needed. The contingency site should house backup PCC software, a copy of the PCC SOP (Standard Operating Procedures) on your LAN or a duplicate CD of the SOP, and a listing of the FRBC Customer Support phone numbers .

Scanner Imaging or Check Reading Problems

If the scanner beeps three times when scanning an image, please check the following:

- Check is inserted with the front facing the center of the scanner (see picture earlier in the *Daily Processing* section).
- Check is inserted right-side up with the MICR line at the bottom.
- Check contains any creases, tears or marks, or the MICR line is unreadable. If so, please ask the customer for another check (if the customer is present). If the customer is not present, try to flatten check or fold it in the opposite direction so it lays flat and try scanning again.

If all of the above are not problems, do the following:

- Unplug the scanner from the outlet, wait 5 seconds, then plug the cord back into the outlet.
- Scan the check at least 2 times.
- Scan another check to ensure that it is not a particular unreadable item.

If you are unable to connect to the scanner or the scanner light is red, please check the following:

- Cable is connected firmly in the back of the scanner and in the serial port of the laptop or tower.
- Replace the RS232 cable with your backup scanner cable.
- Cable is in the correct port on the scanner and laptop.
- Correct COMM port is selected in the POS software under configuration.
- Scanner is more than four inches from any electromagnetic device. These devices include the computer, credit card reader devices, laser beams from bar code scanner devices, etc.
- Scanner is plugged in. (Amber light indicating power up).

If you are still having difficulty, please contact the system administrator. If the system administrator cannot resolve problem, move to the backup scanner and call the FRB PCC Helpdesk to report the problem. A replacement scanner may need to be shipped.

Printer Problems

If experiencing problems with printing, check the following:

- LAN is operational
- Printer is selected from the PCC POS configuration reports
- Printer has paper
- Printer is plugged in
- Printer is online
- Correct printer driver was installed
- Printer is connected to the LAN or to the local printer port on the back of the laptop/desktop
- No paper is jammed in the paper feed tray or the paper output tray

If all of the above are not problems, turn the printer off, wait 5 seconds, then turn it back on.

Contact the system administrator if unable to resolve problem. Connect a local printer if the LAN connection cannot be resolved.

Error Messages

If an error message displays that is not indicated in this Troubleshooting section, or if you are experiencing additional problems, please contact the FRB Customer Service at 800-624-1373 or 216-579-2112 or DSN 510-4-2-86824, option 6, option 4.

If an option is grayed out, you do not have access to perform the action. Contact your system administrator to proceed.

POS Application Error Messages

System Component	Message	Action
Startup sequence	"Only one instance of this application can be running at any given time!"	Click OK. Click on the Windows task bar at the bottom to maximize the application.
	"Please use Control Panel to add a printer to the PC."	Exit application Add a printer to the PC in the operating system.
	"There must be at least one printer configured for the PC."	Exit application Add a printer to the PC in the operating system.
	"Encountered a problem activating the application." "Please use administration tool to configure ALC."	Start the SAT application. Login as a user with configuration permissions. Select System Configuration icon Contact FRBC to enter the correct ALC.
	"ALC cannot be blank."	Start the SAT application. Login as a user with configuration permissions. Select System Configuration icon. Contact FRBC to enter the correct ALC.
	"Encountered a problem activating the application." "Check COM port setting/cables."	Verify the following: • Scanner is powered up and the cables are connected. • Proper COM port is selected. In the POS application, go to File|Configuration, then on the Scanner tab set the proper COM port.

System Component	Message	Action
	"Encountered a problem activating the application." "Check keypad connection/power."	Make sure the keypad power is on and the cable to the scanner is secure. Or, if the location is not using the keypad, it may need to be disabled. Refer to *Installation and Configuration* section for Keypad connections.
Run a check	"Failed to run a check." "Please check scanner."	Make sure the scanner is powered up and the cables are connected.
	"A check processing error has occurred. [Bank number check digit failed]" "Please run the check again."	Try to run the check again. Scanner MICR device may be faulty. Try a different check.
	"A check processing error has occurred. [Duplicate detected]" "Please run the check again."	A duplicate check has been found in the current batch. Review batch list for a resolution.
	"A check processing error has occurred. [Blank field detected]" "Please run the check again."	The software detected a field is blank. Try to run the check again. If error message persists, scanner MICR device i is defective. Call FRBC Helpdesk for replacement. Process check manually using process prior to PCC only if backup scanner is not available.
	"A check processing error has occurred. [Reject characters detected]" "Please run the check again."	The software detected unreadable characters. Try to run the check again . If error message persists, scanner MICR device is defective. Process check manually using process prior to PCC only if backup scanner is not available..
	"Failed to display the image."	Maybe scanner problems (Blown imager bulb) Obtain back-up scanner if available. Contact FRBC for replacement procedures.
	'Store Current Item Fail'	The secondary storage media is not recognized by your computer. Open Windows Explorer and ensure that the drive letter for the drive is displayed. i.e., E:\zip; D:\removable disk. If it's not displayed in Windows Explorer, reboot the computer and check Windows Explorer again. Ensure the storage card or zip disk is properly and securely inserted. Remove the smart media device or zip disk and reinsert to try to re-establish the connection. The storage media may not have space to

System Component	Message	Action
		write to it. The activity should erase at the time of transmission. If the activity is not being erased, contact FRBC Customer Service.
Keypad	"Customer validation failed" "The transaction will be cancelled."	Customer failed to confirm dollar amount on Keypad. Start transaction again.
	"Failed to verify the check." "The transaction will be cancelled."	Customer failed to confirm dollar amount on Keypad. Start transaction again.
Void Item	"A problem was detected while attempting to void the selected check."	Repeat Void Check procedures. The back-up storage location may have been changed during the middle of a batch.
Close Batch	"Unexpected error while printing [Batch List]."	Minimize the application. Confirm if a printer has been set up within the operating system environment. If a printer is present then maximize the application and use File|Configuration, then select Reports tab to select the printer. If no printer is present, then the local administrator will need to add the proper printer. Configure a printer and try to print the batch list. If error still occurs, please call FRB Customer Service.
	"There are currently no printers configured."	Minimize the application. Confirm if a printer has been set up within the operating system environment. If a printer is present, then maximize the application and use File|Configuration, then select Reports tab to select the printer. If no printer is present then the local administrator will need to add the proper printer. Configure a printer and try to close the batch again.
	'Batch Close. Transferring files fatal error. The server name could not be resolved'	The system could not find the CIRA server and therefore could not close the batch. Click on Done on the Close Batch window. Contact the system administrator to ensure that proper connectivity to the Internet through the LAN is available. Contact FRBC to determine if site is down.

System Component	Message	Action
	'Mark batch as Closed. Failed to Mark the Batch as Closed. BatchClose: Incomplete.'	The batch item(s) on the hard drive does not match with the mirror image drive or vice versa. Contact FRBC Customer Service
	"You do not have permissions to close batches."	Check to see if this specific user has the appropriate permissions to close a batch. Refer to *User Administration* in the *Installation and Configuration* section.
	"You do not have permission to transmit a batch."	Confirm that the user has permissions to transmit a batch. Refer to *User Administration* in the *Installation and Configuration* section.

System Component	Message	Action
	"Failed to transmit batch."	Verify internet connectivity by attempting to access another external site. Verify that the ALC+2 is correct. Ensure that the URL for Web Image Transfer is correct and the password has not been altered. Re-try sending.
	"Failed to mark batch as transmitted."	Verify internet connectivity by attempting to access another external site. Verify that the ALC+2 is correct. Ensure that the URL for Web Image Transfer is correct and the password has not been altered. Re-try sending the batch.
	"You do not have permission to delete a batch."	Confirm that the user has permissions to delete a batch. Refer to *User Administration* in the *Installation and Configuration* section.
End Of Day	"You do not have permissions to remove expired verification records."	Confirm that the user has permissions to remove expired verification records. Refer to *User Administration* in the *Installation and Configuration* section.
	"You do not have permissions to update LVD records."	Confirm that the user has permissions to update LVD records. Refer to *User Administration* in the *Installation and Configuration* section.
	"Failed to get MVD delta record."	Verify the site is active and that the ALC+2 is correct. Ensure that the URL for Verification Database is correct. Re-try to download the LVD (local verification database).
	"You do not have permissions to remove activity log records."	Confirm that the user has permissions to remove activity log records. Refer to *User Administration* in the *Installation and Configuration* section.
Change	"A batch is currently open."	Cannot have an active batch and change

Mode	"You must close the current batch in order to change modes."	modes. Close the current batch then try changing modes again.
Tools| Update Check Verification Database	"Update Local Verification Database" "Failed to update LVD."	Confirm Communications. 128 bit encryption - Internet Explorer® 6.0 or higher (recommended browser) - Netscape® 6.2 or higher - Operating system with service pack 2 or higher - Ensure that the URL for the verification database is correct.
	"You do not have permissions to update LVD records."	Confirm current user has permissions to update the LVD records. Refer to *User Administration* in the *Installation and Configuration* section.

SAT Application Error Messages

System Component	Text	Action
User Information	"You do not have permissions to add a role to the system."	Confirm that the user has permissions to configure roles. Refer to *User Administration* in the *Installation and Configuration* section.
	"Change Roles" "Cannot change role of administrator account."	A user cannot change the role for an administrator account. This is by design.
Login	"Access Failed! Please ensure your login and password are correct."	Incorrect user login ID.
	"User Information validation failed." "Login" "The login contains too many characters."	A user must enter a login name less than the maximum. The login is not case sensitive and must be no more than twenty characters. Retype login and select apply.
	"User Information validation failed." "Login" "The login contains too few characters."	A user must enter a login name more than the minimum. The login is not case sensitive and must be at least four characters. Retype login and select apply.
	"User Information validation failed." "Full Name" "The Full Name cannot be blank."	The Full Name field cannot be blank when adding a user. Type in a Full Name without commas or apostrophes and select apply.

® Internet Explorer is a registered trademark of Microsoft Corporation
® Netscape is a registered trademark of Netscape Communications Corporation

	"User Information validation failed." "Password" "The password cannot be empty."	The password field cannot be blank when adding a user. Type in a password and select apply.
	"User Information validation failed." "Password" "The password contains too few characters."	A user must enter a password with a minimum of eight alphanumeric characters, which are case sensitive, then select OK.
	"User Information validation failed." "Password" "The confirmation password does not match the password."	Make sure the user has entered the password correctly twice. Retype both passwords and select the apply button.
	"User Information validation failed." "Roles" "At least one role must be selected."	User must select one role. Refer to *User Administration* in the *Installation and Configuration* section.
	"Failed to apply the changes." "At least one permission must be assigned to a role."	Confirm that the user selected a permission of the role. Then select the apply button. Refer to *User Administration* in the *Installation and Configuration* section.

System Component	Message	Action
	"Failed to apply the changes." " DeleteRolePermission" "Check Permissions."	Confirm the user has permissions to configure roles within the POS application. Refer to *User Administration* in the *Installation and Configuration* section.
	"Encountered a problem creating a new permission." "You do not have permissions to add a role to the system."	Confirm the user has permissions to add roles within the POS application. Refer to *User Administration* in the *Installation and Configuration* section.
	"Encountered a problem deleting a system role." "You do not have permissions to delete a role from the system."	Confirm the user has permissions to delete roles within the POS application. Refer to *User Administration* in the *Installation and Configuration* section.
	Delete role 'rolename'." "Permission denied." "Roles that have been assigned to Users may not be deleted."	Make sure the role to delete is not assigned to a user. 1. Reassign a different role to any user currently using the role desired to be deleted 2. Try to delete the role.
	"The print job '%' was unsuccessful."	Confirm network/local printer is powered up. Confirm that the printer is configured in the operating system environment and a test page can be printed. Confirm that the printer is configured in the

		POS application.

Closing a Batch

If you are unable to close a batch, please check the following:
- LAN cable is plugged securely into the laptop.
- Network is operational.
- Internet connection is successful. Log on to the Internet using Internet Explorer or Netscape and try to go to a site outside of your agency. If this is unsuccessful, contact the system administrator regarding the inability to connect to the web.
- Proper Web site address has been entered. In the PCC SAT, select 'File', 'Configuration', then the 'Image upload' tab. This address field should read 'https://www.mvd.gov/webcontext/jndiSoapSB/jndiSoapSB.wsdl..
- Secondary image storage location is connected. On occasion, smart card media can become loose and needs to be secured again. Eject, then reinsert the media.
- User roles have not been changed. Contact the System Administrator to determine if the user's role has been updated/changed. Have a different user with batch transmission access logon and try to transmit the batch. If the batch transmission is successful, the user's role may have been modified and the user does not have batch transmission access. If needed, request that the user's role be updated to enable batch transmission.

If you are still having difficulty, please contact the system administrator or FRBC.

LAN Connectivity Unavailable

If the LAN is not available, a batch cannot be transmitted.

1. You may continue to process until your network is available, but if you have been using a LAN printer, you might need to install a local printer in order to balance your end-of day transactions .
2. For assistance in installing a local printer, please contact the system administrator or FRBC.
3. Once LAN connectivity is reestablished, the cashier should print the Batch List and Close the Batch.
   NOTE: When the Batch List is printed, it will contain checks from all cashiers which have processed checks since the last successful batch close. The batch listing will print a separate list for each cashier logon utilized, with a Grand Total showing on the last page.

Problem Accessing the CIRA/MVD

If a user experiences difficulty in obtaining images and information from the CIRA/MVD site:

- Try to access another web site to ensure that Internet access is available.
- Shut the computer down and restart it using the 'Shut Down' option from the 'Start' menu. If still unable to access the site but able to access other sites, contact the system administrator.
- Ensure you type the correct password as it is case sensitive. If the account is locked, call FRBC customer service at 800-624-1373, 216-579-2112, or DSN 510-4-2-86824, press 6 then 4.or send an email to PCC@clev.frb.org.

Adjusting an Incorrect Cashier Entry

NOTE: The minimum limit for reporting items that need to be adjusted by FRB Cleveland is $25.00. If the adjustment is $25.00 or more, the check will only be corrected to the written dollar amount on the face of the check.

Prior to Batch Transmission from POS to CIRA

*Scenario 1 – The Cashier entered the incorrect dollar amount, but has not closed the daily batch.

Mistake discovered <u>Prior</u> to transmission to the FRB:
1. Mistake is discovered.
2. Cashier alerts supervisor.
If Point of Sale (POS) Mode:
    3. Customer is contacted and instructed to return with an additional check for the correct amount.
    4. Check is voided within the POS software following SOP procedures for voiding a check.
    5. New check is scanned and entered with the correct dollar amount.
    6. Cashier balances and closes batch.
If Lockbox Mode:
    3. Obtain item from daily work.
    1. Void item with incorrect dollar amount.
    2. Rescan item for correct dollar amount.

*Scenario 2 – The Cashier entered the incorrect dollar amount, but has not closed his/her daily batch.

Mistake discovered (POS mode) <u>Prior</u> to transmission to the FRB and <u>Cannot</u> contact customer:
1. Mistake is discovered.
2. Cashier alerts supervisor.
3. Check is printed within the POS software.
4. Check is voided within the POS software following SOP procedures for voiding a check.
5. Check is sent through the collection system as a paper instrument with agencies reverting to pre-PCC procedures.
Lockbox mode – If the above situation occurs in the Lockbox mode, follow the procedures for 'Voiding a check'.

Prior to Batch Transmission from CIRA to FRBC (FED-ACH)

*Scenario 3 – The cashier entered the incorrect dollar amount, did not properly balance, and transmitted his/her daily batch.

Mistake Discovered <u>After</u> transmission to the FRB:

1. Mistake is discovered.
2. Cashier alerts supervisor.
3. Customer is contacted and instructed to return with an additional check for the amount of the shortage difference or to obtain money if the cashier has an overage.
4. If necessary, new check is scanned and entered.
5. Cashier balances and closes batch. (Cashier will be out of balance for the day by a compensating amount equal to the original out of balance.)

   If the customer cannot be contacted:
6. Complete and submit incident report, reflecting the problem, action taken to this point, and indicating what action is required by FRB-Cleveland.
7. FRB-Cleveland will process an ACH credit to the customers account for the incorrect amount.
8. FRB-Cleveland will process through the paper check copy from CIRA for collection.
9. Completed incident report will be forwarded to FMS and agency personnel.

After Batch Transmission to FRBC (FED-ACH)

Scenario 4 – The cashier entered the incorrect dollar amount, did not properly balance, and transmitted his/her daily batch. Before the mistake was discovered, the daily file was sent from the CIRA to the FRBC.

Mistake Discovered After Fed-ACH file has been created and sent:
Follow procedures in Scenario 3.

Reset or Unlock User Password

Unlock, Activate or Deactivate
If a user has 3 unsuccessful login attempts, their account will become 'Locked'. An administrator can 'Unlock' a user account. (Note: the user's password will also need to be reset – see Reset Password). A user account can also be 'Deactivated' if, for example, a user is on vacation or medical leave. Upon their return, their account can be 'Reactivated'. These functions can only be performed from the User Administration screen. There are no menu options for these functions

1. From the main PCC SAT screen, select the User Administration icon.

2. The screen will display all users as seen below. When a user account is locked a red 'lock' will appear to the left of the login name. When a user id deactivated it will be flagged with a red arrow symbol.

Deactivated   **Locked**

3. To unlock, activate, or deactivate a user account, right-click on the user's login. A drop down menu will appear with choices as seen below.

4. Click the action you wish to take and the user's account is immediately updated.

Reset password

If a user has become locked because they can't remember their password, the administrator needs to unlock the user account, and will also need to reset the user's password.

1. Click the 'User Administration' icon from the main PCC SAT screen. A window will appear that displays all user accounts. Double-click the user login and type a new password in the 'Password' and 'Confirm Password' fields. Passwords requirements mandate that the password have a minimum of eight alphanumeric characters. The password is also case sensitive.
2. The user's role can also be changed on this screen by clicking the new role.
3. When complete, click Apply and Close to exit.
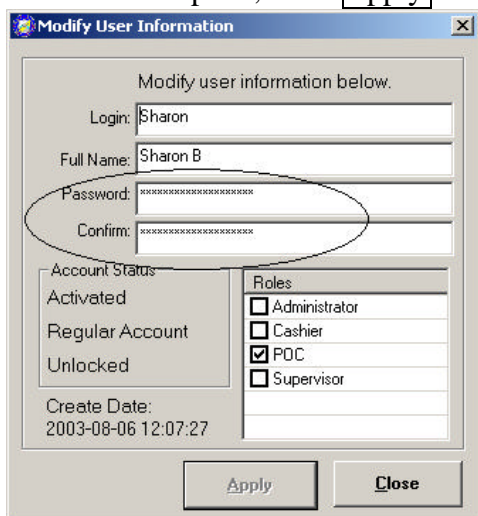
Refilling the Void Stamp

When the 'Void/Electronically Processed' or 'Void/ Non-Negotiated' stamps need refilled, do the following:

1. Press the white section down just a bit, then push the two buttons located on either side of the stamp until they lock-in, which sets the swivel stamp in a locked position as shown below.

2. The ink pad has black ridges that are seen running lengthwise. Using a pencil or ruler, gently push on the black ridge section to slide the ink pad out of the stamping device. The ink pad will slide all the way out of the stamp.

3. Add ink drops onto the ink pad.

4. Slide the ink pad back in all the way with the ink side facing the bottom of the stamp, and the flat bottom of the ink tray resting on the white bridge inside of the bay where it is stored. Activate the ink pad by pressing it down onto a piece of paper.

Local Verification Database (LVD) Reset – if applicable

If an agency is utilizing the check verification process through the LVD download, there will be occasions where a new LVD is required. Daily LVD downloads contain only new items received by the MVD. If there is a change in the location's policy, or if the POS is re -deployed to a new location, an entire new LVD should be obtained.

The LVD reset button erases everything on the LVD in anticipation for relocation. **If the LVD reset is selected and a new LVD is not obtained, there will not be any verification of checks presented.**

To perform an LVD Reset and to obtain a current LVD:
1. Launch the PCC SAT application from the desktop
2. Select the LVD Reset icon from the main SAT screen.
3. Launch the PCC POC application from the desktop.
4. Select 'Tools', then 'Update Check Verification Database…' from the menu to obtain the up-to-date LVD.

United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Personnel Change Over

Revised October 8, 2003

Personnel Change Over

Personnel Change Over

NOTE: Access should be changed on all equipment and backup equipment.

Follow the following procedures for access changes to the POS, MVD and CIRA:

POS Access

When a **system administrator** is replaced, access to the POS needs to be given to the new system administrator. The existing system administrator must logon with "admin" as the user, and select Change Password. The new system administrator then enters the new password for the system administrator role. Once the new replacement has reset "admin", they may create, edit or delete users on that PCC terminal. The resetting of the "admin" password will need to be completed on each PCC terminal. PCC terminals are not linked together and do not share password files.

(Note: Once the administrative password has been changed, it should be written down and locked up for future use. If, at any time, the PCC SAT system cannot be accessed via the administrative logon because the password is not known, the only way to access the SAT is to uninstall and reinstall the PCC POS software. Keeping track (and tight security) of the administrative password is crucial.) It is very important to remember that the "admin" user ID will only be used in an emergency situation and not be used as a daily logon ID.

When POS **user** is replaced, the system administrator must set up logon ID's on the POS for the new user. The new user then enters the new password. For users that no longer exist, an authorized user should remove those users.

MVD and CIRA Access

If applicable, access to the CIRA and MVD needs to be given to the new system administrator. Personnel no longer needing access to your site's business activity need to be removed.

A Change Request Form (see *Appendix*) must be completed and submitted to the Federal Reserve Bank of Cleveland as indicated on the form. The Change Request Form can also be used to request additions or deletions to the current range of ID's and passwords for the CIRA and MVD.

Approximately every six months an email will be sent to the individual that authorized the Change Request Form to verify he/she is still at the same location and a change has not occurred.

Daily Reports

Daily reports, i.e., SF215 and/or SF5515, are emailed on a daily basis to specific contact people at your location. If there is a change to the people who currently receive these emails, a notification of that change must be emailed to PCC@clev.frb.org.

United States Treasury

Financial Management Service

Paper Check Conversion

SOP and User's Manual

Version 2.3.0.2838

Appendix

Revised October 8 , 2003

Table of Contents

Appendix A – Sample Reports

Batch List

The Batch List is a report generated in the POS application by each cashier as the batch is closed and transmitted to the CIRA. A batch list may be created at any time before the batch is closed in addition to being created during the batch close process. The columns on the report found on the next page represent:

- IRN – The unique transaction ID within the POS application. This number follows all transactions through the CIRA and to the Federal Reserve Bank of Cleveland for tracking purposes. The scanner assigns this number as the check is processed. This number is sequential, however unsuccessful scans will result in skipped IRN numbers.
- Date/Time – The date and time that the check is captured, in local time.
- Bank Number – The routing and transit number (also known as the ABA number) found on the MICR line of the check.
- Account Number – The account number at the financial institution as found on the MICR line of the check.
- Check Number – The number on the check, as found on the MICR line of the check.
- Amount – The dollar amount of the check that the cashier entered into the POS application.
- Configurable Fields – The configurable field data specific to each agency.

Batch Totals summarize the following:
- Approved – Successful check transaction
- Void – Voided checks
- Total – Total approved transmission amount (the number of items includes the approved and voiced items).
-

NOTE: Batches can consist of more than one cashier or POS operator, but not of more than one processing mode. If a batch includes checks processed by more than one cashier, each cashier's items will appear on separate pages with that cashier subtotal count and dollar amount. A total count and dollar amount for all cashiers appears on the last page of batch list.

Activity Log and User Information

Activity Log

The Activity Log is an audit trail of activities that occur in the POS and SAT application. Each login and logout is recorded along with the events that occur while a user is signed in. This includes but is not limited to checks scanned, checks voided, and error messages. To view the POS activity log select View Log from the main POS screen. To view the SAT activity log, select the Activity Log icon from the SAT main screen

To print either activity log:
1. Select the event types, sources, and modules desired.
2. Enter the date range. The beginning date should be the last date the log was printed, and the ending date should be the current date.
3. Select Print at the lower right of the screen.

POS Activity Log Report
The fields found on this report include:
- Date/Time – The date and time that the event was recorded, based on the laptop's clock setting.
- Module – The module used.
- Description – The description of the event being logged. (Error messages tend to have more description than what is displayed on the screen during an error condition.)

Page 1

Activity Log

Date: 2002-07-16 16:06:13

ALC: 0000646901

Mode: POS

Printed By: rodney

Date Time	Module	Description

7/16/2002 4:04:41 PM	DEV	System Error.
		Check comm port setting/cables.
		  User Name : rodney
		  User ID : 6532728A-D532-4C45-B8D1-EA0E85DAE62F
		  Number : 111
		  Source : EnableScanner
		  Description : FAILURE: The scanner cannot complete the requested operation.

7/16/2002 4:04:39 PM	POS	System Error.
		Scanner Error
		  User Name : rodney
		  User ID : 6532728A-D532-4C45-B8D1-EA0E85DAE62F
		  Number : 20002
		  Source : Scanner
		  Description : Error: Service object - Establish Communications with scanner failed.

7/16/2002 4:04:31 PM	LVD	System Warning.
		LVD update required.
		  User Name : rodney
		  User ID : 6532728A-D532-4C45-B8D1-EA0E85DAE62F

SAT Activity Log Report

The fields found on this report include:

- Date/Time – The date and time that the event was recorded, based on the laptop's clock setting.
- Source – The source used.
- Module – The module used.
- Description – The description of the event being logged. (Error messages tend to have more description than what is displayed on the screen during an error condition.)

<div align="center">

Activity Log

Date: 2002-07-16 16:09:07

ALC: 0000646901

Printed By: admin

</div>

Date Time	Source	Module	Description

7/16/2002 4:08:11 PM	PCCSAT	LAM	Login
			Logon method failed.
			   User Name :
			   User ID :
			   User Login : admin
			   Number : -49964
			   Source : Local Access Management Subsystem
			   Description : The system could not log you on.
			Make sure your Login and password are correct.

7/16/2002 11:31:30 AM	PCCSAT	LAM	Check permissions.
			Permission denied.
			   User Name : System Administrator
			   User ID : DA31560D-3281-469A-9E68-5AD919D3FC0D
			   Permission : ConfigureRoles

7/16/2002 11:14:25 AM	PCCSAT	LAM	Login
			Logon method failed.
			   User Name :
			   User ID :
			   User Login : administrator
			   Number : -49981
			   Source : Local Access Management Subsystem
			   Description : Login or password is not correct

User Information

The User Administration screen in the PCC SAT application provides user information including the user name, login, and role. This information should be printed prior to an application upgrade so users can easily be re-entered if needed.

To access the user information:
1. Launch PCC SAT application.
2. Select the User Administration icon to view the user information.
3. Select the Printer icon from the top of the User Administration window .to print all the user information.
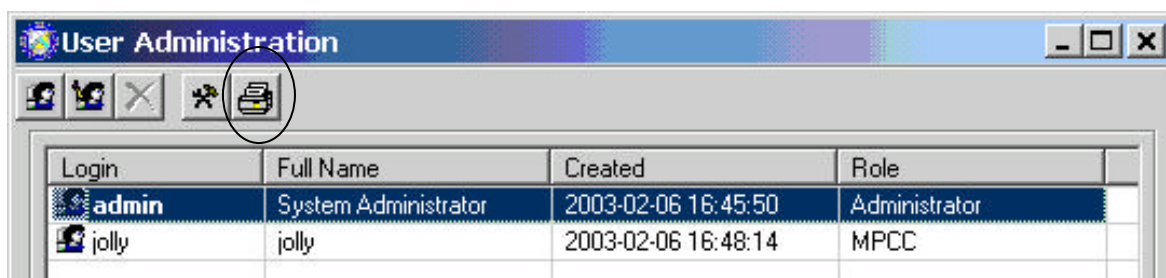
Below is an example of the printout:
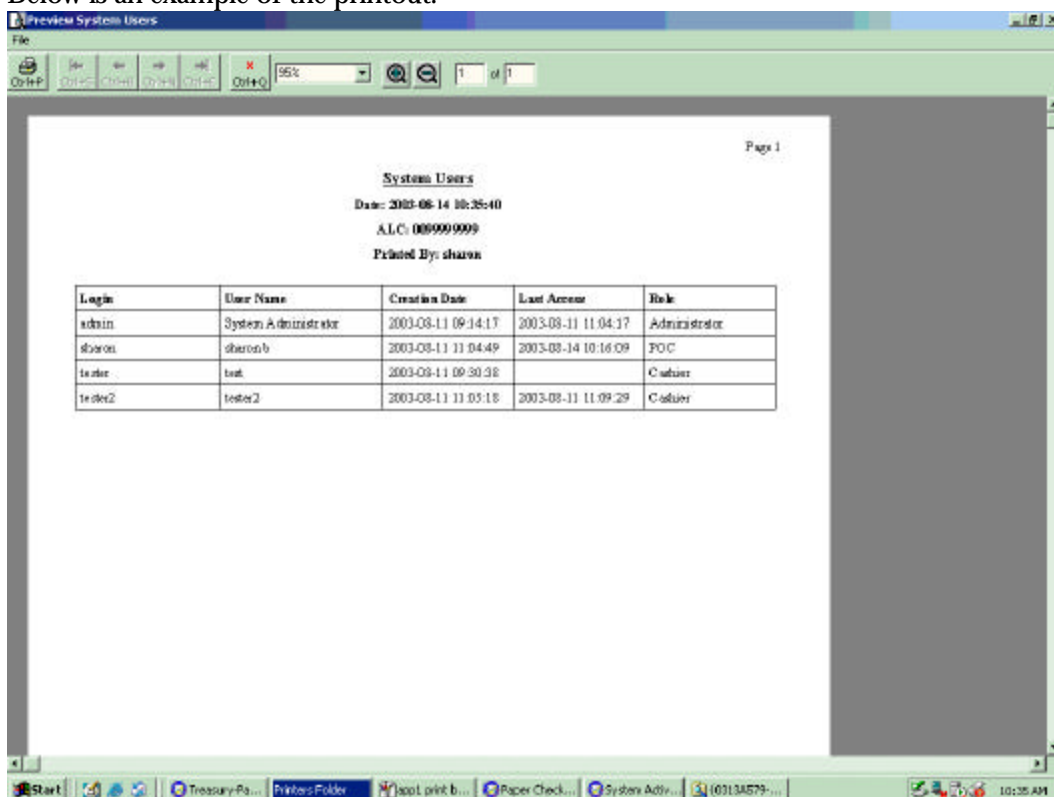
When complete, click Ctrl+Q.

SF215 Deposit Ticket Report

NOTE: If some of the checks cannot be processed electronically and need to be collected through paper check collection channels by the FRB, a separate deposit ticket will be created and reflected in the SF215 report.

The Deposit Ticket Report will be emailed to the designated representative each business day. The information on the report is as follows:

ALC/DSSN – The 9-digit identifier used for accounting purposes to group transactions to a specific battalion. The ninth digit in the ALC is a check digit used only by FRBC. Multiple laptops using the POS application may use the same ALC. The 10 digit ALC + 2 specifies a base or type of location within the ALC and will have a name associated with it.

Deposit Ticket Number – The deposit ticket number as entered into the CashLink system.

Fiscal Agent – This will be the capture center of FRB Cleveland Settlement Date – The date that the transactions are entered into CashLink. The date format is MM/DD/YYYY.

Cashier ID – The cashier ID that processed a group of checks. (If one cashier sends a batch that contains items for multiple cashiers, the individual cashier ID's will not be reflected on the Batch List, however this listing is accurate.)

Transaction Date – The date that the checks were processed. (MM/DD/YYYY)

Summary Count – The total number of checks for a cashier for a specified transaction date.

Summary Amount – The total dollar amount of checks for a cashier for a specified transaction date.

Summary of Transactions – The total number of transactions for all cashiers and all transaction dates that were included in a single CashLink entry.

Summary Total of Dollars – The total dollar amount for the CashLink entry for all cashiers and all transaction dates that were included in a single CashLink entry.

ALC - 000065838	Deposit Ticket # - 0000026	Fiscal Agent - FRB CLEVELAND		Settlement Date - 09/19/2001

215 Detail

ALC - 0000658301   Location Name - BAUMHOLDER, GR

Cashier ID	Transaction Date	Summary Count	Summary Amount
murphyr	09/18/2001	8	$1,950.00
Total ALC - 0000658301		**8**	**$1,950.00**

ALC - 0000658302   Location Name - KAISERLAUTERN, G

Cashier ID	Transaction Date	Summary Count	Summary Amount
LOVEE	09/18/2001	7	$2,575.00
Total ALC - 0000658302		**7**	**$2,575.00**

215 Summary

Summary number of transactions	15
Summary of total Dollars	$4,525.00

SF5515 Debit Voucher Report

The Debit Voucher Report will be emailed to the Financial Officer, or other designated representative on each business day. This report contains the following information:

ALC/DSSN – The 9 digit identifier used for accounting purposes to group transactions to a specific battalion. The ninth digit in the ALC/DSSN is a check digit used only by FRBC.

Fiscal Agent – The Federal Reserve Bank of Cleveland

Return Settlement Date – The date that the return posted to CashLink.

Unique Transaction ID – The IRN number assigned by the scanner that follows each transaction through to the CIRA and FRB Cleveland processing.

Date of Original Transaction – The date that the check was initially processed by the cashier.

Original CashLink DTN – The deposit ticket number (DTN) that contained the original check processed.

$ Amount – The dollar amount of the transaction being returned.

Cashier ID – The Cashier ID that initially processed the check.

5515 - Debit Voucher

ALC - 000065838   **Fiscal Agent -** FRB CLEVELAND   **Return Settlement Date -** 09/06/2001

Debit Voucher Number	Unique Transaction ID	Date of original transaction	Original CA$H-LINK DTN	$ Amount	Cashier ID
0000044	10070150011390000000308	08/27/2001	0000042	$179.66	mkhren6
0000045	10070150011720000000082	08/27/2001	0000042	$683.13	M.Jones
0000046	10070150011720000000083	08/27/2001	0000042	$190.11	M.Jones

Summary number of transactions   3

Summary of total dollars $1,052.90

Pending Redeposit Check Detail Report

The Pending Redeposit Check Detail Report contains information on all items that were returned on the specified day but will be represented later to attempt collection. These items will not result in a SF5515 debit voucher unless all attempts to collect the funds are unsuccessful. This report only identifies items that were returned for non-sufficient funds but will be represented for payment up to 2 times. After two representments, if the check continues to be returned, an SF5515 will be functional. This report contains the following information:

Company ID – The ALC+2 number associated with the location that accepted the original check.

Company Name – The site name associated with the company ID.

Bank Routing - The routing number associated with the ALC, used by the ACH system.

Bank Name – The name of the ALC responsible for these checks.

Unique Transaction ID - The IRN number assigned by the scanner that follows each transaction through to the CIRA and FRB Cleveland processing.

ABA – The routing number that the check was drawn on, as found on the MICR item of the check. In some instances, the ABA number found on the check must be converted to another number due to the item being electronically processed. If that is the case, this is the converted ABA number.

DDA Number – The Demand Deposit Account or checking account number that the check was drawn on, as found on the MICR item of the check.

Amount – The dollar amount of the check.

RTN Date – The date that the item was returned to the Federal Reserve Bank of Cleveland.

Resub Date – The date that the item will be sent back to attempt collection. Under normal circumstances, the check will post to the person's account on the following business day.

Cashier ID – The ID of the cashier that accepted the original check.

RRC – The return reason code, or the reason why the item was returned uncollected. A complete list of return reason codes can be found in Appendix C at the end of this manual.

Company Total Count & Amount – The total number and dollar amount of all return items for a particular ALC +2 location.

Bank Total Count and Amount – The total number and dollar amount of all returns for a particular ALC on a particular day for all of its locations.

```
DATE:     09/07/01                    RETURNWORKS - ACH PROCESSING              CAPTURE CENTER:  FRB
TIME:     10:11:33                 PENDING REDEPOSIT CHECK DETAIL REPORT
                                       From 9/06/2001 To 9/06/2001


COMPANY ID       COMPANY NAME         BANK ROUTING     BANK NAME
0000658302       KAISERLAUTERN, G     041736029        8th Finance Battalion Germany

UNIQUE TRANSACTION ID   ABA         DDA NUMBER              AMOUNT   RTN DATE     RESUB DATE    CASHIER ID           RRC
100701500117200000084   041204823   90-90284                162.72  09/06/2001   09/14/2001    M.Jones              R01
100701500117200000081   241282755   7298                    874.86  09/06/2001   09/14/2001    M.Jones              R09

                                           COMPANY TOTAL COUNT:              2
                                           COMPANY TOTAL AMOUNT:      1,037.58


COMPANY ID       COMPANY NAME         BANK ROUTING     BANK NAME
0000658303       WIESBADEN, GR        041736029        8th Finance Battalion Germany

UNIQUE TRANSACTION ID   ABA         DDA NUMBER              AMOUNT   RTN DATE     RESUB DATE    CASHIER ID           RRC
100701500113900000326   243486067   00064962              1,701.52  09/06/2001   09/14/2001    mkhren6              R09
100701500113900000306   041211382   2309                    198.94  09/06/2001   09/14/2001    mkhren6              R01
100701500113900000310   243486096   0056484267            1,728.91  09/06/2001   09/14/2001    mkhren6              R01

                                           COMPANY TOTAL COUNT:              3
                                           COMPANY TOTAL AMOUNT:      3,629.37


                                             BANK TOTAL COUNT:              5
                                             BANK TOTAL AMOUNT:      4,666.95
```

Appendix B - Return Reason Codes

Return Reason Code (RRC)	Description
R01	Insufficient funds
R02	Account closed
R03	No account/unable to locate account
R04	Invalid account number
R06	Returned per Originating Depository Financial Institution's request
R07	Authorization revoked by customer
R08	Payment stopped
R09	Uncollected funds
R10	Customer advises not authorized
R11	Check truncation entry return
R12	Branch sold to another Depository Financial Institution
R13	RDFI not qualified to participate
R14	Representative Payee (account holder) deceased or unable to continue in that capacity
R15	Beneficiary or account holder (other than a representative payee) deceased
R16	Account frozen
R17	File record edit criteria
R18	Improper effective entry date
R19	Amount field error
R20	Non-transaction account
R21	Invalid company identification
R22	Invalid individual ID number
R23	Credit entry refused by receiver

R24	Duplicate entry
R25	Addenda Error
R26	Mandatory field error
R27	Trace number error
R28	Routing number check digit error
R29	Corporate customer advises not authorized
R30	RDFI not participant in Check Truncation Program
R31	Permissible return entry
AA	Non functioning return reason code
R32	RDFI Non-settlement
R33	Return of XCK Entry
R34	Limited participation DFI
R38	Stop payment on source document
R40	Non participant in ENR program
R41	Invalid Transaction Code (ENR only)
R42	Routing Number/Check digit error
R43	Invalid DFI Account number
R44	Invalid Individual ID Number
R45	Invalid Individual name
R46	Invalid representative payee indicator
R47	Duplicate Enrollment
R50	State law prohibits truncated checks
R51	Notice not provided/signature not authentic/Item altered/Ineligible for conversion
R52	Stop payment on item
R61	Misrouted return
R62	Incorrect Trace number
R63	Incorrect Dollar amount
R64	Incorrect Individual Identification
R65	Incorrect Transaction Code
R66	Incorrect Company Identification
R67	Duplicate Return
R68	Untimely Return

R69	Multiple errors
R70	Permissible return entry not accepted
R71	Misrouted Dishonor return
R72	Untimely Dishonored return
R73	Timely Original Return
R74	Corrected Return
R80	Cross-Border payment Coding error
R81	Non-participant in Cross-border program
R82	Invalid Foreign receiving DFI Identification
R83	R83Foreign Receiving DFI unable to settle

Appendix D – System Administrator Responsibility

The Paper Check Conversion (PCC) program will require the local system Administrator to provide a small, but important, amount of system support at initial deployment. Basic system administrator support will primarily be related to the initial deployment of the system. System administrator support may also be needed for troubleshooting and equipment tracking.

System Administrator Support Prior to Deployment

The system administrator will be responsible for working with the designated agency contact (i.e. Regional Account Manager, Financial Manager, etc, in order to complete the Agency Site Profile (ASP). Generally the ASP will require the system administrator to:
1. Identify the local baseline software and install baseline software as needed.
2. Identify the hardware specifications of any existing computer in the finance cage.
3. Provide a LAN drop for the system if PC is not already connected to the LAN.
4. Reserve an IP address.
5. Other items relating to electrical power.
6. Install Tiff viewer if ActiveX not enabled by your agency.

Basic System Administrator Support at the Time of Deployment

The System Administrator is responsibility for the following at the time of deployment:
1. Install the local baseline software package, hot fixes, and user settings if not done prior to deployment.
2. Assign an IP address to the computer and make it a member of the local network.
3. Ensure that the computer has access to the Internet (usually through the LAN) at 128 bit encryption.
4. Set up the computer to print out on the network printer (or local printer if no network printer is available).
5. Set up the designated agency contact and Cashiers to have read/write access to the RDM folder on the hard drive and have permissions set to all access to the network printer.
6. Ensure that the hard drive is NTFS configured, if applicable.
7. Request copy of PCC software from deployment specialist.
8. Ensure that the computer has a secondary storage unit such as a zip drive or PCMCIA storage card (if not supplied by the FRBC)

Continuing System Administrator Support

See the *Troubleshooting* section for hardware issues pertaining to the PCC computer and scanner.

FOR ALL OTHER ISSUES PLEASE CONTACT YOUR AGENCY PCC POINT OF CONTACT OR CALL THE FEDERAL RESERVE BANK OF CLEVELAND AT 216-579-2112, OR 800-624-1373 OR SEND AN EMAIL TO PCC@CLEV.FRB.ORG.

Appendix E – Equipment Returns

Use the following address for returning laptops and scanners using certified mail return receipt or FedEx. Please include a note of explanation with the damaged or defective equipment. Insurance needs to be utilized during the shipping process for the full amount of the equipment. Contact the PCC Helpdesk for a dollar valuation of the equipment you are returning.

PCC Deployment Center
Federal Reserve Bank of Cleveland
1455 E. 6th Street – Ground Floor, Main Building
Cleveland, OH   44114

Appendix F – Change Request Form

Please complete the Change Request form on the next page when there is a position change over. It can also be used to request additions or deletions to the current range of ID's and passwords for the CIRA and MVD.

Appendix G – MVD/CIRA Change Request

Paper Check Conversion
Master Verification Database /Central Image and Research Archive
Change Request – This also will need to be replaced!

Agency:_____ **Eight Digit ALC or DSSN**: _____

Instructions:
Please specify the Paper Check Conversion (PCC) system for which this change is requested and then complete the form below as appropriate to the type of modification required. Please note, all changes must be approved by the senior officer or manager and then mailed to the Federal Reserve Bank of Cleveland.

PCC System: ___ Master Verification Database or ___ Central Image and Research Archive
Or _____Master Verification Database Reports or ____ Central Image and Research Archive Reports

___

__ ADD   ___ PERSONNEL CHANGE FOR USERID:_____
(List specific UserID)
The following party has been designated as a PCC user for this location. The individual listed below has agreed not to disclose his/her password to others, and has been advised that he/she is responsible for all actions related to the use of his/her ID within the PCC system. He/she also understands that unauthorized disclosure of any PCC information may be cause for loss of access and disciplinary action.

_____   _____
Name (printed or typed)   Rank / Title

_____   _____
Signature   Last Four Digits of SSN

_____   _____
E-mail   Phone (Commercial)

_____   _____
FAX   Phone (DSN Country Code)

_____   _____   _____
Address (Country and APO if applicable)   City / State   Country / Zip

MVD Role: ___View ___Edit   _____
                                                                Sites to be Viewed (Central Image and Research Archive users)
Access will remain in effect until notice is provided to the Federal Reserve Bank of Cleveland.

__ DELETE:

UserID: _____   Name: _____
                                                                                   (printed or typed)
_____

Approved by: _____ _____
                        Senior manager   Date

                  _____
                        Name & Title (printed or typed)

            _____   _____
                        E-mail   Phone (Commercial and DNS Country Code)

                        Return this form to: Federal Reserve Bank of Cleveland ;P.O. Box 6387,
                        Cleveland Ohio 44101-1387 Attn: Information Security Department ;FAX: 216-579-3175

Appendix H – Hand Receipt

The hand receipt on the next page should be completed at the time of installation to verify receipt of equipment. Please complete the form and return it to the deployment specialist, or fax to 216-579-2125, Attn: Federal Reserve Bank of Cleveland, PCC Deployment Team.

Hand Receipt

Paper Check Conversion

| To: Company/Agency: Location: Phone:		Hand Receipt number:
Serial/Stock number:	**Item Description:**	**Quantity:**
	TOTAL:	

Hardware received by:

_____
Signature

_____
Date

Please give the completed form to the Deployment Specialist,
or Fax to 216-579-2125, Attn: Federal Reserve Bank of Cleveland, PCC Deployment Team

Appendix I – Overview of System Administration Tool (SAT)

The PCC SAT application icon, located on the desktop, is used to complete security and application configuration setup by authorized users.

The PCC-SAT application consists of the following components:
- System Configuration – Used to configure the POS application, including System Access, System Activity, Verification Database, Secondary Image Storage, System Parameters, and POS Connections.
- User Administration – Setting up, editing and deleting users, including user role configuration.
- Activity Log – A view of all actions performed in the SAT.
- Batch Recovery – Used to retrieve a batch from the secondary storage in the case of an unexpected terminal failure
- LVD Reset – If utilizing the Verification Database, the LVD reset button erases everything on the LVD in anticipation for a replacement with new data.
- Help - Provides the SAT version and system information.

System Configuration   User Administration   Activity Log   Batch Recovery   LVD Reset   Help
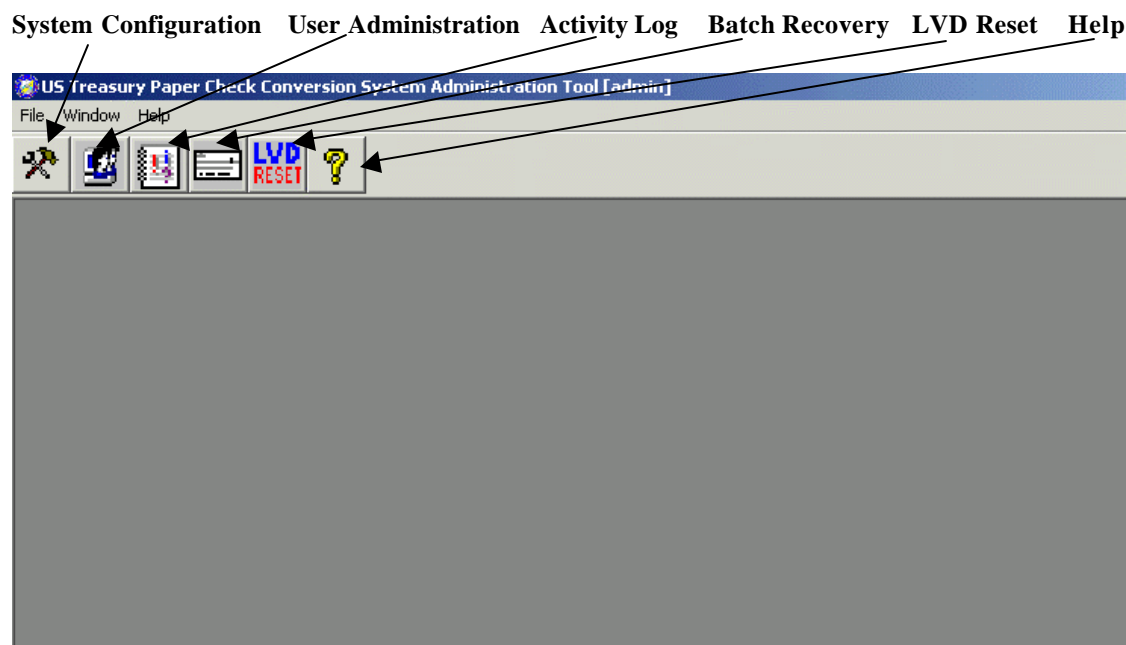
Appendix J - System Permission Descriptions

Permission	Description
AuthorizeOldVerification	Authorize the use of an out-of-date LVD
BrowseBatches	Browse through batches in the system
ChangeOwnPassword	Change own password
CloseBatch	Close a batch
ConfigurePOS	Configure the POS application with an ALC, Terminal ID and OwnerCode
ConfigureRoles	Change role configuration
ConfigureSystem	Change system configuration (e.g. COM+ constuctor string)
ConfigureUser	Perform user configuration functions
DeleteBatches	Delete batches
DeleteExpiredReturns	Delete expired LVD returns
LimitActivityLog	Limit old activity log records
OverrideVerification	Override a deny, returned from the verification system
ProcessTransactions	Process transactions at the POS
RecoverFromSecondaryStorage	Recover the database from the data stored in the Secondary storage location
ResetLVD	Reset local verification database
TransmitBatch	Transmit a closed batch to a remote site
UpdateLVD	Update the LVD
ViewActivityLog	View activity log entries
ViewBatchList	View the list of entries in a batch
VoidTransaction	Void a previously processed transaction

Appendix K – Add Blocked Record Request for MVD

Please complete the *Add Blocked Record Request for MVD* form on the next page when a person, account number or routing number needs to be blocked through the verification database.

Paper Check Conversion
Add Blocked Record Request for MVD

Requestor:

Name:

Title:

Phone Number:

Email:

Agency/ALC:

Block Transaction Information:

RT:

Account #:

Config. Field 1:

Reason for Block:

Block Placement Level:

ALC:
ALC+2:

Authorization for Block:

senior officer or manager signature

Print Name:

Title:

Location:

FMS Use Only	*FRB Use Only*
Approved By:	Input By:
	Name Date
Date Approved:	Verified By:
	Name Date

For any questions, please email pcc@clev.frb.org
Please return this form to:
Financial Management Service
Attn: Reggie McKinney
Fax: (202) 874-8644
Email: Reginald.McKinney@fms.treas.gov
Address: 401 14th Street SW Room 508D
Washington, DC 20227

Appendix N – RDM Scanner Information

Refer to the RDM EC5000I User Manual for more detailed information on the PCC scanner.